现代数学基础丛书

有限群导引

下册

● 徐明曜 黄建华 李慧陵 李世荣 著



科学出版社

现代数学基础丛书

有限群导引

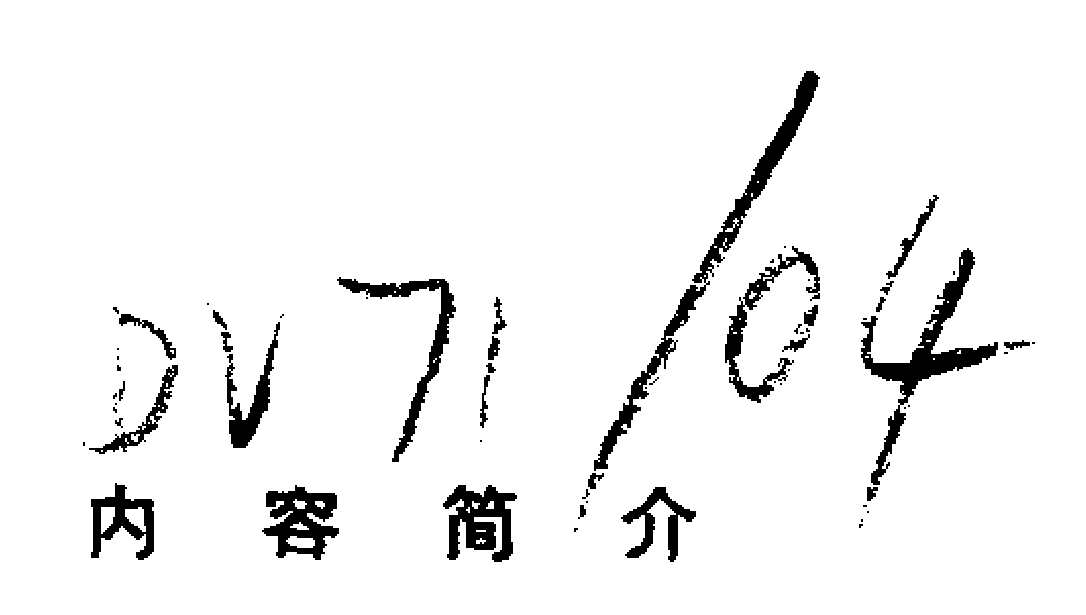
下册

徐明曜　黄建华
李慧陵　李世荣　著

科学出版社

1999





内 容 简 介

本书分上下册出版.下册内容共分八章,第七章到第十章继续讲述抽象群的理论,包括群上的作用, 幂零群,可解群和 群的进一步知识.第十一、十二两章分别介绍典型群和置换群的基本知识,这对于有限群的应用是非常基本的.第十三章讲当代最新发展有限群的几何理论.最后一章讲群论在图论中的应用.

本书内容简明而翔实,特别注意有限群的应用方法.包含相当数量的习题,书末有解答和提示.

本书适合于高校数学、物理和化学专业研究生、教师和有关科技工作者阅读.

图书在版编目(CIP)数据

有限群导引(下)/徐明曜等著. -北京:科学出版社,1999.3

(现代数学基础丛书/程民德主编)

ISBN 7-03-007196-4

Ⅰ.有… Ⅱ.徐… Ⅲ.有限群 Ⅳ.O152.1

中国版本图书馆 CIP 数据核字(98)第 38371 号

科学出版社 出版

北京东黄城根北街 16 号

邮政编码:100717

新蕾印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1999 年 5 月第 一 版	开本:850×1168 1/32
1999 年 5 月第一次印刷	印张:13 1/8
印数:1-2 000	字数:345 000

定价:27.00 元

下册前言

如上册初版前言所述，本书是作为教材而编写的，目的是用尽量少的篇幅介绍有限群论的基本知识和基本方法，使读完本书的读者能够接触有限群的现代文献，并开始进行一些研究工作.

自本书上册于 1987 年由科学出版社出版以来，已过去了 11 年. 由于作者方面的原因，下册未能及时交稿付排. 在这 11 年间，作者不断收到读者来信询问下册何时出版，也有的要求购买已经售缺的上册，这对我们是很大的鞭策和鼓励. 现在，在科学出版社的帮助下，终于完成了全书的出版工作，我们谨对关心本书的学术界朋友和广大读者，以及科学出版社的同志们表示衷心的感谢.

本书下册共分八章. 第 VII 章到第 X 章继续讲述抽象群的理论. 首先在第 VII 章讲群在群上的作用，这是群的局部分析理论的基础. 第 VIII 章讲 p- 幂零群， Glauberman 的 ZJ- 定理，并且作为这些理论的应用，讲了 Burnside p^aq^b- 定理的群论证明以及 Thompson 的关于 Frobenius 群的 Frobenius 核必为幂零群的著名定理. 之后，在第 IX 章和第 X 章里分别讲述了可解群和 p- 群的进一步知识. 在讲抽象群的四章之后，第 XI 章和第 XII 章分别介绍典型群和置换群的基本知识，这些具体的群的知识是非常基本的，而且对于今天 (单群分类完成之后) 的有限群工作者，特别是想应用有限群的结果到数学的其它领域，譬如几何、组合论以及图论的人们来说是至关重要的. 本书的第 XIII 章讲有限群的几何理论. 1980 年单群分类问题解决之后， J. Tits 所创立的群几何

理论迅速发展，并已成为有限群论的重要组成部分. 近年来，群几何理论向有限群的许多分支渗透，并取得了一些令人瞩目的成果；特别地，群几何理论为最终完成有限单群分类定理的证明，起到了十分重要的作用. 而且目前群几何理论的应用已远远超出了有限群的范围. 本书的最后一章 —— 第 XIV 章讲群论在图论上的应用. 我们在这一章中只讲述了群与图这个广泛的研究领域中的很少几个问题，借以说明群论是如何应用到具有较高对称性的图的理论中去的.

我们认为在下册中，第 VII, VIII, XI, XII 四章是基本的，每个专攻有限群的研究生都应该认真学习. 这四章加上上册的六章可作为硕士生一年的课程. 如感到时间较松，可再选学剩下的四章中的一章到两章. 这可凭借教师的兴趣以及研究生的培养目标而定. 对于这剩下的四章的选材，基本上是根据作者的兴趣，而并不追求内容的完整.

本书下册具有和上册相同的写作特点，初版前言中的 1–5 款仍请读者注意.

下册的写作除了上册作者徐明曜外，又加上了合作者黄建华、李慧陵和李世荣. 其中徐明曜负责第 VII, VIII, X, XIV 四章的写作，李世荣写作第 IX 章，李慧陵写作第 XII 章，而第 XI, XIII 两章由黄建华执笔.

编写本书下册增加了以下四本参考书：

8. M. Suzuki, *Group Theory I*, Springer-Verlag, 1982.

9. M. Suzuki, *Group Theory II*, Springer-Verlag, 1986.

10. M. Aschbacher, *Finite Group Theory*, Cambridge University Press, Cambridge, 1986.

11. H. Kurzweil und B. Stellmacher, *Theorie der endlichen Gruppen*, Springer-Verlag, 1998.

限于作者的水平，本书还会有错误和不足之处，亟盼读者给以指正.

最后，我们要感谢首都师范大学王汝楫教授、广西大学班桂宁教授、北方交通大学冯衍全博士、郑州大学王长群博士、清华

大学王殿军博士以及北京大学博士生曲海鹏，他们对本书的初稿进行了校对，并协助进行计算机排版的工作．特别是王汝楫教授和曲海鹏同学，他们认真阅读了本书大部分章节，提出了不少修改的意见．

徐明曜 黄建华

李慧陵 李世荣

1998 年 8 月于北京大学

目　录

第 VII 章

群在群上的作用

我们在第 II 章中研究了群在集合上的作用，证明了有限群最基本的定理 —Sylow 定理. 第 VI 章又讲述了群表示论，它研究的是群在向量空间上的作用. 应用这个理论可以得到十分丰富的结果. 本章我们将讨论群在群上的作用，这时作用的对象是另一个群. 从某种意义上来说，它似乎介于群在集合上的作用和群在向量空间上的作用两者之间. 因为群虽然比集合有更丰富的代数结构，但又远不及向量空间，后者是一个以域为算子集的交换群. 因此，我们企望能从这种研究中得到某些新的概念，方法和结果. 它不象在集合上的作用那样空泛，同时又能把表示论的某些结果和方法应用到远更广泛的场合，这种想法从逻辑上看是合理的，而且在实际上也已经取得了丰硕的成果. 事实上，从 50 年代末开始创立的研究有限群的群论方法 (或更精确地，局部分析方法) 正是以此为基础的.

我们知道，群元素在集合上的作用相当于该集合的一个置换，它在向量空间上的作用相当于该空间的满秩线性变换，而它在群上的作用则相当于该群的一个自同构. 因而, 本章也可以看成是对自同构群的进一步研究. 由于这几种作用的对象迥然不同，因此，所考虑的中心问题以及得到的结果也很不一样. 但尽管如此，它们都以一个统一的“作用”的观点为中心，这个观点是十分重要的. 如果我们把视野再扩大一些，允许群作用的集合有某种几何的或组合的结构，比如它们是图，射影平面，或区组设计

等，那么还会得到许多令人惊异的结果，无论是对群还是对这些组合结构.

以上这些话我们希望能对读者学习和研究有限群提供某些方法性的启示.

§1. 群在群上的作用

定义 1.1 设 G 和 H 是给定的有限群. 若 φ 是 H 到 $\mathrm{Aut}(G)$ 内的一个同态映射. 我们就称 φ 为 *H 在 G 上的一个作用*.

于是，对于任意的 $h \in H$, 有 $\varphi(h) \in \mathrm{Aut}(G)$. 并且对于任意的 $g \in G$, 我们以 g^h 表 g 在 $\varphi(h)$ 之下的像，即规定 $g^h = g^{\varphi(h)}$.

和第 II 章以及第 VI 章的情形相同，我们称 φ 为*忠实作用*, 如果 $\mathrm{Ker}\,\varphi = 1$; 而称 φ 为*平凡作用*, 如果 $\mathrm{Ker}\,\varphi = H$, 这时有 $\varphi(H) = 1$.

根据第 III 章讲述的群扩张理论，由群 G, H 和作用 φ 可唯一确定一个 G 和 H 的半直积 $S = G \rtimes_\varphi H$. 在 S 中，$h \in H$ 在 G 上的作用就相当于共轭变换，亦即 $g^h = h^{-1}gh$, $\forall g \in G$. 显然，半直积 S 是直积当且仅当 φ 是平凡作用.

例 1.2 设 S 是群，$H, G \leq S$, 且 $H \leq N_S(G)$. 则 *H 在 G 上的共轭作用是 H 在 G 上的一个作用.*

这个作用虽然简单，但非常重要. 它和上述作半直积的考虑恰好相反.

定义 1.3 设 φ 是群 H 在 G 上的一个作用，$A \leq G$, 称 A 为 *H-不变的*, 如果 $A^h \subseteq A$, $\forall h \in H$.

事实上，因为 h 在 A 上的作用相当于 A 的自同构，$A^h \subseteq A$ 等价于 $A^h = A$. 因而在上述定义中可用 $A^h = A$ 代替 $A^h \subseteq A$.

如果在半直积 $S = G \rtimes_\varphi H$ 中考虑，G 的子群 A 是 H-不变的就等价于 $H \leq N_S(A)$. 因而 “A 是 H-不变的” 也常称作 “A 被 H 正规化”.

定义 1.4 设 φ 为 H 在 G 上的一个作用. 如果 G 中存在非平凡的 H-不变子群, 则称作用 φ 为 **可约的**, 否则称为 **不可约的**.

又, 如果 G 可表成两个非平凡的 H-不变子群 A, B 的直积 $G = A \times B$, 则称作用 φ 为 **可分解的**, 否则称为 **不可分解的**.

命题 1.5 *设 φ 是群 H 在 G 上的作用.*

(1) 若 A 是 G 的 H-不变子群, 则 $C_G(A)$ 和 $N_G(A)$ 也是 G 的 H-不变子群.

(2) 若 A 是 G 的 H-不变正规子群, 则 φ 诱导出 H 在 G/A 上的作用 $\bar{\varphi} : h \mapsto \bar{\varphi}(h)$, 这里 $\bar{\varphi}(h) : gA \mapsto g^h A$, $\forall g \in G$.

证 (1) 首先看一个一般性的结论. 设 A, G 是群 S 的子群, 且 $A \leq G$, α 是 S 的自同构. 则易验证

$$C_G(A)^\alpha = C_{G^\alpha}(A^\alpha), \quad N_G(A)^\alpha = N_{G^\alpha}(A^\alpha). \tag{1.1}$$

(例如验证后者: 由 $g \in N_G(A) \iff g \in G$ 且 $g^{-1}Ag = A \iff g^\alpha \in G^\alpha$ 且 $(g^\alpha)^{-1}A^\alpha g^\alpha = A^\alpha \iff g^\alpha \in N_{G^\alpha}(A^\alpha)$, 即可得到 $N_G(A)^\alpha = N_{G^\alpha}(A^\alpha)$.)

下面把 (1.1) 式应用到本命题: 设 S 为半直积 $G \rtimes_\varphi H$, $h \in H$. 命 α 为由 h 诱导出的 S 的内自同构, 注意到 $A^h = A$, $G^h = G$, 则可由 (1.1) 式得到

$$C_G(A)^h = C_{G^h}(A^h) = C_G(A),$$

$$N_G(A)^h = N_{G^h}(A^h) = N_G(A).$$

再由 h 的任意性, 即得 $C_G(A)$ 和 $N_G(A)$ 是 G 的 H-不变子群.

(2) 设 $g, g' \in G$, $gA = g'A$, $h \in H$. 由 $gA = g'A$, $g^{-1}g' \in A$. 于是 $(g^{-1}g')^h \in A^h = A$, $(g^h)^{-1}g'^h \in A$, 即 $g^h A = g'^h A$. 故映射 $\bar{\varphi}(h)$ 是有意义的. 注意到上述过程可以逆推, 故 $\bar{\varphi}(h)$ 是 G/A 到自身的单射. 因当 g 跑遍 G 时 g^h 亦跑遍 G, 故 $\bar{\varphi}(h)$ 又是满射. 而 $\bar{\varphi}(h)$ 保持运算是明显的, 这样 $\bar{\varphi}(h) \in \mathrm{Aut}(G/A)$. 最后, 对于 $h, h' \in H$, 因为

$$(gA)^{\bar{\varphi}(hh')} = g^{hh'}A = (g^h A)^{\bar{\varphi}(h')} = (gA)^{\bar{\varphi}(h)\bar{\varphi}(h')},$$

故 $\bar{\varphi}(hh') = \bar{\varphi}(h)\bar{\varphi}(h')$. 于是 $\bar{\varphi}$ 是 H 到 $\mathrm{Aut}(G/A)$ 内的同态. □

下面我们推广已经熟悉的中心化子和换位子的概念.

定义 1.6 设群 H 作用在群 G 上.

(1) 规定 $C_G(H) = \{g \in G \mid g^h = g, \ \forall h \in H\}$, 即 $C_G(H)$ 为 H 在 G 中的不动点的集合. 显然, $C_G(H)$ 是 G 的 H-不变子群.

(2) 设 $g \in G$, $h \in H$, 规定

$$[g,h] = g^{-1}g^h.$$

同时规定

$$[G,h] = \langle [g,h] \mid g \in G \rangle,$$
$$[G,H] = \langle [g,h] \mid g \in G, h \in H \rangle.$$

事实上, 如果在半直积 $S = G \rtimes_\varphi H$ 中考虑, 上述概念即我们所熟知的中心化子和换位子的概念. 仿照换位子群, 以下我们还约定

$$[G,H,H] = [[G,H],H], \qquad [G,h,h] = [[G,h],h],$$

等等.

命题 1.7 *设群 H 作用在 G 上. 则 $[G,H]$ 是 G 的 H-不变正规子群, 且 H 在 $G/[G,H]$ 上作用平凡. 又若 N 是 G 的一个 H-不变正规子群, 使得 H 在 G/N 上作用平凡, 则 $[G,H] \le N$.*

证 对于任意的 $g, g_1 \in G$, $h, h_1 \in H$, 有

$$\begin{aligned} [g,h]^{h_1} &= [g^{h_1}, h^{h_1}] \in [G,H], \\ [g,h]^{g_1} &= [gg_1, h][g_1, h]^{-1} \in [G,H]. \end{aligned}$$

故 $[G,H]$ 是 G 的 H-不变正规子群. 又因

$$(g[G,H])^h = g^h[G,H] = g[g,h][G,H] = g[G,H],$$

故 H 在 $G/[G,H]$ 上作用平凡.

现在假定 N 是 G 的 H-不变正规子群, 且对任意的 $h \in H$, $g \in G$ 有

$$(gN)^h = g^h N = gN,$$

则 $g^{-1}g^h N = N$, 即 $[g,h] \in N$, 于是 $[G,H] \le N$. □

命题 1.8 *设有限 p-群 H 作用在有限 p-群 $G \neq 1$ 上, 则有 $C_G(H) \neq 1$, 且 $[G,H] < G$.*

证 这时半直积 $S = G \rtimes H$ 也是有限 p-群. 因为 $G \lhd S$, 有 $1 \neq Z(S) \cap G \le C_G(H)$, 故 $C_G(H) \neq 1$. 又因 S 幂零, $[G,S] < G$, 当然更有 $[G,H] < G$. □

定理 1.9 *设 p-群 H 作用在群 G 上, 则存在 $P \in \mathrm{Syl}_p(G)$ 是 H-不变的.*

证 令 $S = G \rtimes H$, 取 $R \in \mathrm{Syl}_p(S)$ 满足 $H \le R$. 则若令 $P = R \cap G$, 有 $P \in \mathrm{Syl}_p(G)$. 最后因

$$P^H = (R \cap G)^H = R^H \cap G^H = R \cap G = P,$$

故 P 是 H-不变的. □

§2. π'-群在交换 π-群上的作用

前面说过, 群的表示也可以看成是群在群上的作用, 只不过被作用的群是一个向量空间的加法群. 因此, 表示论的方法和结果对于一般地研究群在群上的作用应该有它的应用. 在表示论中, 如果域的特征等于零或者不整除所讨论的群的阶, 其理论有它的简便之处. 这提示我们, 在研究群在群上的作用时也应该先加上类似的假设, 这就是假定作用的群和被作用的群的阶是互素的, 也就是研究 π'-群在 π-群上的作用, 这里 π 是一个素数集合. 另外, 交换群比非交换群更接近于向量空间, 因此我们先来研究 π'-群在交换 π-群上的作用.

这时，在表示论中起重要作用的 Schur 引理和 Maschke 定理都有它们的推广了的形式.

定理 2.1 (Schur 引理) *设 φ 是群 H 在交换群 G 上的一个不可约作用，又设 $E = \mathrm{End}(G)$ 是 G 的自同态环. 则 $C_E(\varphi(H))$ 是一个体.*

证 不失普遍性，可设 φ 是忠实作用. 即可设 $H \leq \mathrm{Aut}(G) \subseteq E$. 我们来证明 $C = C_E(H)$ 是一个体.

容易验证 C 是 E 的一个子环. 于是我们只须再证明 C 中每个非零元素 α 都是可逆的，并且其逆 $\alpha^{-1} \in C$ 即可.

考虑 $\mathrm{Ker}\ \alpha$ 和 G^α. 我们来证明它们都是 G 的 H-不变子群. 设 $h \in H$, $k \in \mathrm{Ker}\ \alpha$, 有 $(k^h)^\alpha = (k^\alpha)^h = 1$, 故 $k^h \in \mathrm{Ker}\ \alpha$. 这得到 $\mathrm{Ker}\ \alpha$ 的 H-不变性. 再设 $g \in G$, 由 $(g^\alpha)^h = (g^h)^\alpha \in G^\alpha$, 又得到 G^α 的 H-不变性. 现在由 $\alpha \neq 0$ 以及 φ 是不可约作用，必有 $\mathrm{Ker}\ \alpha = 0$ 和 $G^\alpha = G$. 于是 α 是可逆的，而 $\alpha^{-1} \in C$ 是明显的.
□

定理 2.2 (Maschke) *设 π'-群 H 作用在交换 π-群 G 上，A 是 G 的 H-不变子群，并且是 G 的直因子，即存在 $B \leq G$ 使 $G = A \times B$，则必可找到 G 的某个 H-不变子群 K 使 $G = A \times K$.*

证 令 ρ 是 G 到 A 上的射影. 如下规定 G 到 G 内的另一映射 ψ:

$$g^\psi = \prod_{h \in H} (g^n)^{h\rho h^{-1}},$$

其中 n 是满足 $n|H| \equiv 1 (\mathrm{mod}\ |G|)$ 的一个正整数，这样的 n 存在是因为 $(|G|, |H|) = 1$. 我们有

(1) ψ 是 G 到 A 内的映射：由 A 的 H-不变性.

(2) ψ 是 G 到 A 上的射影：对 $a \in A$ 有

$$a^\psi = \prod_{h \in H} (a^n)^{h\rho h^{-1}} = \prod_{h \in H} ((a^n)^h)^{\rho h^{-1}}$$

$$= \prod_{h\in H}(a^n)^{hh^{-1}} = \prod_{h\in H} a^n$$
$$= a^{n|H|} = a.$$

(3) ψ 是 G 到 A 上的 H-同态, 从而 $K = \operatorname{Ker}\psi$ 也是 G 的 H-不变子群: 对于任意的 $h' \in H$,

$$\begin{aligned} g^{\psi h'} &= \prod_{h\in H}(g^n)^{h\rho h^{-1}h'} \\ &= \prod_{h\in H}(g^n)^{h'(h'^{-1}h)\rho(h'^{-1}h)^{-1}} \\ &= \prod_{h\in H}((g^{h'})^n)^{(h'^{-1}h)\rho(h'^{-1}h)^{-1}} \\ &= \prod_{h'^{-1}h\in H}((g^{h'})^n)^{(h'^{-1}h)\rho(h'^{-1}h)^{-1}} \\ &= g^{h'\psi}, \end{aligned}$$

故 ψ 是 H-同态. 从而 K 也是 G 的 H-不变子群.

(4) $G = A \times K$: 因 ψ 是 G 到 A 上的射影, $A \cap K = 1$. 又对任意的 $g \in G$, 有 $g = g^\psi \cdot (g^\psi)^{-1}g$, 其中 $g^\psi \in A$, 而因 $((g^\psi)^{-1}g)^\psi = ((g^\psi)^\psi)^{-1}g^\psi = (g^\psi)^{-1}g^\psi = 1$, 故 $(g^\psi)^{-1}g \in K$. 定理得证. □

注 2.3 从上述证明可以看出, 在定理的条件中, "G 是 π-群" 可以减弱为 "G 有一个 H-不变直因子 A 是 π-群", 定理的结论仍能成立.

下面来研究 H 在 G 上作用的不可分解性. 我们来证明

定理 2.4 *设 p'-群 H 作用在交换 p-群 G 上. 令 $\Omega = \Omega_1(G)$, 它作为 G 的特征子群当然是 H-不变的. 假定 Ω 是 H-可约的, 则 G 必为 H-可分解的.*

证 设 $\exp G = p^e$, 则 $1 \neq \mho = \mho_{e-1}(G)$. 因为 $\mho \operatorname{char} G$, 故 $\mho$ 是 H-不变的. 又因 Ω 是 H-可约的, 存在它的非平凡 H-不变子群 K. 我们可以选到 $K \le \mho$. (这总是可以办到的. 因为若 $\mho < \Omega$,

则可取 $K=\mho$; 而若 $\mho=\Omega$, 则可任取 Ω 的非平凡 H-不变子群作为 K.) 令 $|K|=p^k$. 再令 T 是 G 的满足 $T\cap K=1$ 的极大 H-不变子群, 当然有 $T\neq 1$. (因为据定理 2.2, 在 Ω 中就有非平凡 H-不变子群与 K 的交为 1.)

考虑 $\overline{G}=G/T$. 由命题 1.4(2), H 也作用在 $\overline{G}$ 上, 并且子群 $\overline{K}=KT/T$ 也是 $\overline{G}$ 的 H-不变子群. 我们有

(1) $\exp\overline{G}=p^e$, $\overline{K}\leq\mho_{e-1}(\overline{G})$ 且 $|\overline{K}|=|K|=p^k$: 因为 $K\leq\mho$, 故对 K 的任一非单位元素 y, 可找到元素 $x\in G$ 满足 $y=x^{p^{e-1}}$, 则 x 在 $\overline{G}$ 中的像 $\bar{x}$ 必满足 $\bar{x}^{p^{e-1}}\neq\bar{1}$. (若否, $\bar{x}^{p^{e-1}}=\bar{1}$, 即 $x^{p^{e-1}}\in T$. 但 $x^{p^{e-1}}\in K$, 故 $x^{p^{e-1}}\in K\cap T=1$, 于是 $x^{p^{e-1}}=y=1$, 矛盾.) 于是有 $\exp\overline{G}\geq p^e$, 但 $\exp G=p^e$, 故 $\exp\overline{G}=p^e$.

又因 $K\leq\mho_{e-1}(G)$, 当然有 $\overline{K}\leq\mho_{e-1}(\overline{G})$, 而因

$$|\overline{K}|=|KT/T|=|K/K\cap T|=|K|,$$

故 $|\overline{K}|=p^k$.

(2) $\overline{G}$ 中不存在与 $\overline{K}$ 不相交的非平凡的 H-不变子群: 若有这样的子群 $\overline{T}_1=T_1/T$, $\overline{T}_1\cap\overline{K}=\bar{1}$, 则由 $T_1\cap K=1$ 及 $T_1>T$, 与 T 的极大性相矛盾.

(3) $\overline{K}=\mho_{e-1}(\overline{G})=\Omega_1(\overline{G})$: 若否, 则必有 $\overline{K}<\Omega_1(\overline{G})$. 于是由定理 2.2, 在 $\Omega_1(\overline{G})$ 中存在非平凡 H-不变子群 $\overline{T}_1$ 满足 $\overline{T}_1\cap\overline{K}=\bar{1}$, 与 (2) 矛盾.

由 (3), $\overline{G}$ 必为 k 个 p^e 阶循环子群的直积. 我们设 $\overline{G}=\langle\bar{a}_1\rangle\times\cdots\times\langle\bar{a}_k\rangle$, a_i 是 $\bar{a}_i$ 的原像, $i=1,\cdots,k$. 并令 $M=\langle a_1,\cdots,a_k\rangle$. 则显然有 $G=MT$. 因为 $o(\bar{a}_i)=p^e$, 必有 $o(a_i)=p^e$, 于是 $M=\langle a_1\rangle\times\cdots\times\langle a_k\rangle$ 的阶为 $p^{ek}=|\overline{G}|$. 故

$$|M|=|G/T|=|MT/T|=|M/T\cap M|,$$

于是 $M\cap T=1$. 这说明了 $G=M\times T$. 因为 T 是 H-不变的, 再用定理 2.2, 即得 G 存在 H-不变子群 M_1 满足 $G=M_1\times T$, 于是 G 是 H-可分解的. □

推论 2.5 *p'-群 H 不可分解地作用在交换 p-群 G 上, 则 G 必为齐次循环 p-群, 即它的型不变量为 $(p^e,p^e,\cdots,p^e)$, 其中 $p^e=\exp G$.*

证 若否，则 $\mho_{e-1}(G) < \Omega_1(G)$. 于是 $\Omega_1(G)$ 是 H-可约的. 应用定理 2.4 即得到矛盾. □

注意，在定理 2.4 和推论 2.5 中 H 是 p'-群的假设是不可少的. 下面的例子说明，若去掉这个假设，这两个结果都不成立.

例 2.6 设 $G = \langle a \rangle \times \langle b \rangle$，其中 $o(a) = p^2$，$o(b) = p$. 映射 $h : a \mapsto ab, b \mapsto b$ 是 G 的一个 p 阶自同构. 令 $H = \langle h \rangle$. 则 H 在 G 上的作用是不可分解的，但 H 在 $\Omega_1(G)$ 上的作用是可约的. (请读者自行验证.)

在下节里我们还要把推论 2.5 的结果推广到 π'-群在交换 π-群上的不可分解作用的情形，参看定理 3.4. 底下我们证明 π'-群在交换 π-群上作用的另一个重要结果.

定理 2.7 *设 π'-群 H 作用在交换 π-群 G 上. 则*

$$G = C_G(H) \times [G, H].$$

证 不失普遍性，可假定 $H \leq \mathrm{Aut}(G)$.

首先，容易验证：如果任一交换群 G 有一幂等自同态 θ, 即满足 $\theta^2 = \theta$ 的自同态 θ,(或任一群 G 有一正规幂等自同态 θ, 即与 G 的每个内自同构可交换的幂等自同态 θ), 则必有

$$G = \mathrm{Ker}\ \theta \times G^\theta,$$

并且若 G 是交换群，则还有

$$\mathrm{Ker}\ \theta = \{g^{-1}g^\theta \mid g \in G\}.$$

更进一步，假定 θ 与 H 的每个元素可交换，则 Ker θ 和 G^θ 都是 G 的 H-不变子群. (验证从略.)

我们令 $\theta = |H|^{-1} \sum_{h \in H} h$, 其中 $|H|^{-1}$ 是满足 $|H|^{-1}|H| \equiv 1 \pmod{|G|}$ 的整数，则有

$$\theta h_1 = |H|^{-1} \sum_{h \in H} hh_1 = \theta = h_1\theta, \quad \forall h_1 \in H,$$

和

$$\theta^2 = \theta(|H|^{-1}\sum_{h\in H} h) = |H|^{-1}\sum_{h\in H}\theta h = |H|^{-1}|H|\theta = \theta.$$

于是 θ 是与 H 中每个元素皆可换的幂等自同态. 由前面所说的, 为完成证明还只须证

$$G^\theta = C_G(H), \qquad \mathrm{Ker}\ \theta = [G,H].$$

设 $x\in C_G(H)$, 则 $x^h = x$, $\forall h\in H$. 于是

$$x^\theta = x^{|H|^{-1}\Sigma_{h\in H}h} = x^{|H|^{-1}|H|} = x,$$

故 $x\in G^\theta$. 而若 $x\in G^\theta$, 则存在 $y\in G$ 使 $x=y^\theta$. 于是

$$x^h = y^{\theta h} = y^\theta = x, \qquad \forall h\in H,$$

故 $x\in C_G(H)$. 这样, 有 $C_G(H)=G^\theta$. 又设 $[g,h]\in[G,H]$, 其中 $g\in G$, $h\in H$. 则

$$[g,h]^\theta = (g^{-1}g^h)^\theta = (g^\theta)^{-1}g^{h\theta} = (g^\theta)^{-1}g^\theta = 1,$$

故 $[g,h]\in \mathrm{Ker}\ \theta$. 由 g, h 的任意性得 $[G,H]\le \mathrm{Ker}\ \theta$. 反过来, 对于 $\mathrm{Ker}\ \theta$ 中的任一元素 $g^{-1}g^\theta$, 其中 $g\in G$, 有

$$\begin{aligned} g^{-1}g^\theta &= g^{-1}g^{|H|^{-1}\Sigma_{h\in H}h} = \prod_{h\in H}(g^{-1}g^h)^{|H|^{-1}} \\ &= \prod_{h\in H}[g,h]^{|H|^{-1}} \in [G,H], \end{aligned}$$

故 $[G,H]=\mathrm{Ker}\ \theta$. □

有了这个定理, 我们可以证明

推论 2.8 *设 H 是交换 p-群 G 的 p'-自同构群, 如果 H 在 $\Omega_1(G)$ 上作用是平凡的, 则 $H=1$.*

证 设 $C = C_G(H)$, $D = [G, H]$. 则由定理 2.7 有 $G = C \times D$. 于是 $\Omega_1(G) = \Omega_1(C) \times \Omega_1(D)$. 又由假设有 $\Omega_1(G) \leq C$, 于是 $\Omega_1(G) \leq \Omega_1(C)$, 这迫使 $\Omega_1(D) = 1$, 于是 $D = 1$. 这样有 $G = C_G(H)$, 即 $H = 1$. □

在 §4 中我们还要把这个结果推广到非交换 p-群上去.

§3. π'-群在 π-群上的作用

本节研究 π'-群在一般的 (不一定交换的)π-群上的作用. 从内容上说它大体可分为三部分: 首先研究这种作用的可约性和可分解性问题; 然后证明几个一般性的结果; 最后讨论交换 π'-群 H 在 π-群 G 上的作用, 研究 H 的非单位元的不动点的性质.

在本节的讨论中, Schur-Zassenhaus 定理起着基本的作用.

引理 3.1 *设 π'-群 H 作用在 π-群 G 上, G 和 H 中至少有一个可解, 素数 $p \mid |G|$. 则 G 中存在 H-不变的 Sylow p-子群, 并且 G 的任二 H-不变的 Sylow p-子群在 $C_G(H)$ 下共轭.*

证 令 $P \in \mathrm{Syl}_p(G)$. 考虑半直积 $S = G \rtimes H$. 由 Frattini 论断, 有 $S = GN_S(P)$. 于是

$$H \cong S/G = GN_S(P)/G \cong N_S(P)/N_G(P).$$

由 Schur-Zassenhaus 定理, $N_S(P)$ 中存在 $N_G(P)$ 的补 K, 并且它也是 G 在 S 中的补, 于是有 $H = K^g$, 对某个 $g \in G$ 成立. 因为 K 正规化 P, 故 H 正规化 P^g, 即 P^g 是 G 的 H-不变 Sylow p-子群.

现在设 P_1 和 P_2 是 G 的两个 H-不变的 Sylow p-子群. 则存在 $x \in G$ 使 $P_1^x = P_2$. 于是 $N_S(P_2)$ 包含 H^x 和 H. 由 Schur-Zassenhaus 定理, 存在 $y \in N_G(P_2)$ 使 $H^x = H^y$. 于是 $H^{xy^{-1}} = H$, 并且 $P_1^{xy^{-1}} = P_2$. 因为对任一 $h \in H$ 有 $[xy^{-1}, h] \in H \cap G = 1$ 于是 $xy^{-1} \in C_G(H)$, 引理证毕. □

注 3.2 在引理 3.1 中，条件"G 和 H 中至少有一个可解"是多余的. 因为由 Feit-Thompson 定理，奇数阶群是可解的，而因 $(|G|,|H|)=1$, G 和 H 中至少有一个是奇数阶的，因而是可解的. 一个有趣的问题是在引理 3.1 中去掉 G 和 H 有一个可解的条件来寻求一个不依赖于 Feit-Thompson 定理的证明.

定理 3.3 *设 π'-群 H 不可约地作用在 π-群 G 上，则 G 是初等交换 p-群.*

证 首先，G 必为 p-群. 若否，则由引理 3.1, 有 G 的 Sylow p-子群 P 是 H-不变的，与不可约性相矛盾. 其次，因为 $\Phi(G)\ \mathrm{char}\ G$, $\Phi(G)$ 必为 G 的 H-不变子群. 又因 $\Phi(G)<G$, 由 G 的不可约性必有 $\Phi(G)=1$, 于是 G 为初等交换 p-群. □

回忆一下，一个有限 p-群叫做齐次循环 p-群，如果它是若干个同阶循环 p-群的直积.

定理 3.4 *设 π'-群 H 不可分解地作用在交换 π-群 G 上，则 G 必为齐次循环 p-群.*

证 首先，G 必为 p-群. 若否，则由定理 3.1, 有 G 的 Sylow p-子群 P 是 H-不变的. 因为 G 是交换群，P 显然为直因子，于是由定理 2.2, G 可分解为 P 与另一 H-不变子群的直积，与 G 的不可分解性相矛盾. 至此，再用推论 2.5, 即得所需之结果. □

下面我们转而讨论 π'-群在 π-群上作用的一般性质，它们在以后的讨论中是非常重要的.

定义 3.5 设 G 是群，$H\le \mathrm{Aut}(G)$. *我们称 H 固定 G 的子群列*

$$G=G_0\ge G_1\ge\cdots\ge G_s=1, \tag{3.1}$$

如果对 $i=0,1,\cdots,s-1$, 有 $[G_i,H]\le G_{i+1}$.

这时，因为对每个 $g\in G_i$, $h\in H$, 有 $[g,h]=g^{-1}g^h\in G_{i+1}\le G_i$, 故 $g^h\in G_i$, 于是每个 G_i 都是 G 的 H-不变子群.

定理 3.6 设 G 是 π-群， $H \le \mathrm{Aut}(G)$. 如果 H 固定 G 的子群列 (3.1), 则 H 亦为 π 群.

证 我们只须证明 H 的任一 π'-元素 h 必等于 1. 用对子群列的长 s 的归纳法，可设 $[G_1, h] = 1$. 现在假定 $o(h) = n$, 则由 h 是 π'-自同构，有 $(n, |G|) = 1$. 对于任意的 $g \in G$, 我们有 $g_1 = [g, h] = g^{-1}g^h \in G_1$, 而 $g^h = gg_1$, 由此推出

$$g^{h^2} = (gg_1)^h = g^h g_1 = gg_1^2.$$

同理可推出 $g^{h^3} = gg_1^3, \cdots, g^{h^n} = gg_1^n$, 因为 $h^n = 1$, 故得 $g = gg_1^n$, 即 $g_1^n = 1$. 由 $(n, |G|) = 1$ 得 $(n, o(g_1)) = 1$, 于是得 $g_1 = 1$, 这样有 $g^h = g$, $\forall g \in G$, 即 $h = 1$. □

推论 3.7 设 π'-群 H 作用在 π-群 G 上，如果 H 固定 G 的子群列 (3.1), 则 H 在 G 上作用平凡.

下面的引理对底下的讨论是十分重要的.

引理 3.8 设群 H 作用在群 G 上. 若 G 有一个 H-不变子群 A 满足 $(|H|, |A|) = 1$, 且 $(Ag)^h = Ag$, $\forall h \in H$. 则存在 $x \in Ag$ 使 $x^h = x$, $\forall h \in H$.

证 考虑半直积 $S = A \rtimes H$. 对任意的 $a \in A$, $h \in H$, 因 $h^{-1}(ag)h \in Ag$, $h^{-1}a(ghg^{-1}) \in A$. 于是 $ghg^{-1} \in HA = S$, $gHg^{-1} \le S$. 由 Schur-Zassenhaus 定理， H 和 gHg^{-1} 在 S 中共轭，即存在 $a_1 \in A$ 使 $a_1^{-1}Ha_1 = gHg^{-1}$, 即 $(a_1g)H(a_1g)^{-1} = H$. 于是，对任意的 $h \in H$, 有 $h^{-1}(a_1g)h(a_1g)^{-1} \in H$. 另一方面，因 $h^{-1}(a_1g)h \in Ag$, 故 $h^{-1}(a_1g)h(a_1g)^{-1} \in A$. 由 $A \cap H = 1$, 得 $h^{-1}(a_1g)h(a_1g)^{-1} = 1$. 于是取 $x = a_1g$, 即得 $x^h = x$, $\forall h \in H$. □

定理 3.9 设 π'-群 H 作用在 π-群 G 上， N 是 G 的 H-不变的正规 π-子群，则 $C_{G/N}(H) = C_G(H)N/N$.

证 显然， $C_G(H)N/N \le C_{G/N}(H)$. 反过来，设 $Ng \in C_{G/N}(H)$, 由引理 3.8 存在 $x \in C_G(H)$ 使 $Ng = Nx$, 于是 $Ng \in C_G(H)N/N$, 定理得证. □

定理 3.10 设 π'-群 H 作用在 π-群 G 上，则

$$G = C_G(H)[G,H].$$

证 因为 $[G,H]$ 是 G 的 H-不变正规子群，且 H 在 $G/[G,H]$ 上作用平凡，于是 $C_{G/[G,H]}(H) = G/[G,H]$. 由定理 3.9 有

$$C_G(H)[G,H]/[G,H] = C_{G/[G,H]}(H).$$

于是得 $G = C_G(H)[G,H]$. □

定理 3.11 设 π'-群 H 作用在 π-群 G 上，则

$$[G,H,H] = [G,H].$$

特别地，如果 $[G,H,H] = 1$, 则 $[G,H] = 1$, 即 H 在 G 上作用平凡.

证 显然 $[G,H]$, $[G,H,H] = [[G,H],H]$ 和 $C = C_G(H)$ 都是 H-不变的. 由定理 3.10 有 $G = C[G,H]$, $[G,H] = (C\cap[G,H])[G,H,H]$, 于是有 $G = C[G,H,H]$. 设 g 是 G 的任意元素，则有 $g = cx$, 其中 $c \in C$, $x \in [G,H,H]$. 于是对任意的 $h \in H$, 有 $g^{-1}g^h = x^{-1}c^{-1}c^hx^h = x^{-1}x^h$. 因为 $x \in [G,H,H]$, $[G,H,H]$ 是 H-不变的，有 $x^{-1}x^h \in [G,H,H]$, 于是有 $[G,H] \subseteq [G,H,H]$. 反过来，因为 $[G,H]$ 是 H-不变的，显然有 $[G,H,H] \subseteq [G,H]$, 于是得 $[G,H] = [G,H,H]$. □

下面的 Thompson 引理是十分重要的.

引理 3.12 设 $H = A\times B$ 是 p-群 G 的一个自同构群，其中 A 是 p'-群，而 B 是 p-群. 如果 $C_G(A) \geq C_G(B)$, 则 $A = 1$.

证 因为 $C_G(B)$ 在 A 和 B 之下都不变，当然也在 $H = A\times B$ 下不变. 设 $Q \geq C_G(B)$ 是 G 的使 A 在其上作用平凡的极大阶 H-不变子群，我们要证明 $Q = G$, 于是有 $A = 1$. 若否， $Q < G$,

则因 G 是 p-群，$N_G(Q) > Q$, 并且 $N_G(Q)$ 也是 G 的 H-不变子群.

在 $N_G(Q)$ 中取真包含 Q 的 G 的极小 H-不变子群 S. 令 $\overline{S} = S/Q$. 因为 $\Phi(\overline{S})$ char $\overline{S}$, $\Phi(\overline{S})$ 自然也是 $\overline{S}$ 的 H-不变子群. 由 S 的极小性必有 $\Phi(\overline{S}) = \overline{1}$, 于是 $\overline{S}$ 是初等交换 p-群. 因为 B 也是 p-群，B 在 $\overline{S}$ 上的作用必有不动点，即 $C_{\overline{S}}(B) \neq \overline{1}$. 又因为 $[A, B] = 1$, 易验证 B-不变子群 $C_{\overline{S}}(B)$ 也是 A-不变的，从而是 H-不变的. 再由 S 的极小性，就有 $C_{\overline{S}}(B) = \overline{S}$, 即 $[S, B] \leq Q$. 因 $[Q, A] = 1$, 有

$$[S, B, A] = 1.$$

又因 $[B, A] = 1$, 有

$$[B, A, S] = 1.$$

根据三子群引理，得

$$[A, S, B] = 1.$$

即 $[S, A] \leq C_S(B) \leq C_G(B) \leq Q$. 于是 A 固定群列

$$S > Q \geq 1.$$

由推论 3.7, A 在 S 上作用平凡，与 Q 的极大性矛盾. □

作为 Thompson 引理的应用，我们证明关于 p-可解群的一个结果，它在第 IX 章 §1 中将要用到.

定理 3.13 *设 B 是 p-可解群 G 的一个 p-子群. 令 $C = C_G(B)$, $N = N_G(B)$. 则*

$$O_{p'}(N) \leq O_{p'}(G), \qquad O_{p'}(C) \leq O_{p'}(G).$$

证 因为 $O_{p'}(C)$ char C, $C \lhd N$, 故 $O_{p'}(C) \lhd N$, 于是 $O_{p'}(C) \leq O_{p'}(N)$. 因此我们只须对 N 证明定理的结果.

先设 $O_{p'}(G) = 1$. 令 $A = O_{p'}(N)$. 注意到 A, B 均在 N 中正规，得 $[A, B] = 1$. 令 $A \times B$ 依共轭变换作用在非平凡 p-子群 $P = O_p(G)$ 上. 因为 $C_P(B) \leq C_G(B) = C \leq N$, 而 $A \lhd N$, 则

$C_P(B)$ 正规化 A, 即 $[C_P(B),A] \leq A$. 又 $[C_P(B),A] \leq [P,A] \leq P$, 于是 $[C_P(B),A] \leq A \cap P = 1$. 这推出 $C_P(A) \geq C_P(B)$. 据引理 3.12, 有 $A \leq C_G(P)$. 又因 G 是 p-可解群且 $O_{p'}(G) = 1$, 由第 V 章习题 6, 有 $C_G(P) \leq P$, 于是 $A \leq P$. 但 A 是 p'-群, P 是 p-群, 故必有 $A = 1$. 即 $O_{p'}(N) \leq O_{p'}(G) = 1$.

现在假定 $Q = O_{p'}(G) \neq 1$. 令 $\overline{G} = G/Q$, $\overline{B} = BQ/Q$. 于是 $O_{p'}(\overline{G}) = \overline{1}$. 而前面已证 $O_{p'}(N_{\overline{G}}(\overline{B})) = \overline{1}$. 据第 II 章命题 2.6, 有 $N_{\overline{G}}(\overline{B}) = N_G(B)Q/Q$. 于是 $O_{p'}(NQ/Q) = \overline{1}$, 即 $O_{p'}(NQ) \leq Q$, 最终得到 $O_{p'}(N) \leq Q = O_{p'}(G)$. □

在本节的最后, 我们研究交换 π'-群在 π-群上的作用. 最重要的结果是下面的

定理 3.14 *设交换 π'-群 H 作用在 π-群 G 上, 则*

$$G = \langle C_G(A) \mid A \leq H, \text{ 且} H/A \text{ 循环} \rangle.$$

证 不失普遍性, 可设 $H \leq \mathrm{Aut}(G)$. 设 G 是使定理不真的极小阶反例. 则有

(1) $G_1 = \langle C_G(A) \mid A \leq H, \text{ 且} H/A \text{ 循环} \rangle < G$;

(2) 若 $U < G$, $U^H = U$, 则 $U \leq G_1$;

(3) 若 $1 \neq N \lhd G$, $N^H = N$, 则 $N = G$.

其中 (1) 表明 G 是反例, (2) 由 $|G|$ 的极小性得到. 为证明 (3), 我们设 $N \neq G$. 由 (2) 有 $N \leq G_1$. 于是由 $|G/N| < |G|$ 及 $|G|$ 的极小性有

$$G/N = \langle C_{G/N}(A) \mid A \leq H, \text{ 且} H/A \text{ 循环} \rangle.$$

据定理 3.9, $C_{G/N}(A) = C_G(A)N/N$. 故

$$G/N = \langle C_G(A)N/N \mid A \leq H, \text{ 且} H/A \text{ 循环} \rangle = G_1/N.$$

于是 $G = G_1$, 矛盾.

现在设 $p \mid |G|$. 由引理 3.1, G 中存在 H-不变的 Sylow p-子群 P. 如果 G 不是 p-群, 则 $P < G$. 由 (2), $P \leq G_1$. 再由 p 的任意

性，有 G 的任一 Sylow 子群含于 G_1，于是 $G = G_1$，矛盾．故 G 必为 p-群．又因 $\Phi(G) \lhd G$, $\Phi(G)^H = \Phi(G)$，由 (3) 有 $\Phi(G) = 1$，即 G 是初等交换 p-群，并且 H 在 G 上作用不可约．据 Schur 引理 (定理 2.1)，有 $\mathbf{F} = C_{\mathrm{End}(G)}(H)$ 是一个体．因为 $|G|$ 有限，$\mathbf{F}$ 是有限体，因而是域 (Wedderburn 定理)．又由 H 是交换群有 $H \leq \mathbf{F}$．但域的乘法群的有限子群皆为循环群，这样 H 是循环群．取 $A = 1$，于是 $G_1 \geq C_G(1) = G$，矛盾． □

推论 3.15 *设交换但非循环的 π'-群 H 作用在 π-群 G 上，则*

$$G = \langle C_G(x) \mid x \in H - \{1\} \rangle.$$

证 因为 H 非循环，若 H/A 循环，则必有 $A \neq 1$．取 $x \in A - \{1\}$，则 $C_G(x) \geq C_G(A)$．于是可由定理 3.14 推出所需的结果． □

§4. Hall-Higman 简化定理和 Blackburn 定理

假定 π'-群 H 非平凡地作用在 π-群 G 上，则总存在 G 的这样的 H-不变子群 G_1，使得 H 在 G_1 上作用非平凡，但在 G_1 的每个 H-不变真子群上作用平凡．所谓 Hall-Higman 简化定理就是研究这样的临界群 G_1 的性质．

定理 4.1 (Hall-Higman) *设 π'-群 H 非平凡地作用在 π-群 G 上，但平凡地作用在 G 的每个 H-不变的真子群上．则 G 是 p-群，并且有*

(1) H 不可约地作用在 G/G' 上，且

$$[G, H] = G, \quad C_G(H) = G', \quad C_{G/G'}(H) = \bar{1};$$

(2) 若 G 交换，则 G 为初等交换 p-群；而若 G 非交换，则 $G' = Z(G) = \Phi(G)$；

(3) $Z(G)$ 是初等交换 p-群；

(4) 若 $p \neq 2$，则 $\exp G = p$.

证 设 $p \mid |G|$, 则由引理 3.1, 存在 G 的 H-不变的 Sylow p-子群 P. 如果 G 不是 p-群, 则由定理假设, H 在 P 上作用平凡. 因为对于 $|G|$ 的每个素因子, 都可找到一个这样的 Sylow 子群, 它们生成整个的群 G, 而这将推出 H 在 G 上作用平凡, 与假设矛盾. 故 G 必为 p-群.

(1) 由定理 3.10, $G = [G, H]C_G(H)$. 若 $[G, H] < G$, 则由假定 H 在 $[G, H]$ 上作用平凡. 又显然 H 在 $C_G(H)$ 上作用平凡, 这将推出 H 在 G 上作用平凡, 矛盾. 故必有 $[G, H] = G$.

令 $\overline{G} = G/G'$, 则由 $[G, H] = G$ 有 $[\overline{G}, H] = \overline{G}$. 据定理 2.7, $\overline{G} = [\overline{G}, H] \times C_{\overline{G}}(H)$, 于是 $C_{\overline{G}}(H) = \bar{1}$. 又由定理 3.9,

$$C_{\overline{G}}(H) = C_{G/G'}(H) = C_G(H)G'/G',$$

故 $C_G(H) \le G'$. 再由 $\Phi(G)$ char G, $\Phi(G)$ 是 G 的 H-不变真子群, 于是 $\Phi(G) \le C_G(H)$. 注意到 $G' \le \Phi(G)$, 这就迫使 $C_G(H) = G' = \Phi(G)$.

最后, 对于 $\overline{G}$ 的 H-不变真子群 $\overline{N}$, 由定理条件有 H 在 $\overline{N}$ 上作用平凡, 即 $\overline{N} \le C_{\overline{G}}(H)$. 但 $C_{\overline{G}}(H) = \bar{1}$, 故 $\overline{N} = \bar{1}$, 即 H 在 $\overline{G}$ 上作用是不可约的.

(2) 设 G 交换, 则由 (1), H 在 G 上作用是不可约的. 于是由定理 3.3, G 必为初等交换 p-群. 假定 G 不交换, 即 $G' \ne 1$. 前面已证 $G' = \Phi(G)$. 又因 $Z(G)$ char G, 故 $Z(G)$ 是 G 的 H-不变真子群, 于是 $Z(G) \le C_G(H) = G'$. 为证明 $Z(G) = G'$, 我们用反证法. 假定 $Z(G) < G'$, 必有 $D = C_G(G') < G$. 因 D 是 H-不变的, 由定理假设, H 在 D 上作用平凡. 考虑 D 用共轭变换作用在 G 上. 而在半直积 $G \rtimes H$ 中, 又可认为 $D \times H$ 作用在 G 上. 这时有 $C_G(H) \ge C_G(D)$. (若否, 因为 $C_G(D)$ 是 H-不变的, 则由定理条件必有 $C_G(D) = G$, 即 $D \le Z(G)$. 据 IV, 定理 2.10(2), 有 $Z_2(G) \le D$, 于是有 $Z_2(G) \le Z(G)$, 这将迫使 G 交换, 矛盾.) 应用引理 3.12, 得到 H 在 G 上作用平凡, 矛盾. 于是必有 $Z(G) = G'$.

(3) 若 G 交换, 当然有此结论. 若 G 不交换, 则有 $c(G) = 2$. 于是对任意的 $a, b \in G$, 有 $a^p \in \Phi(G) = Z(G)$, 这推出 $[a^p, b] =$

$[a,b]^p = 1$. 再由 $G' = Z(G)$ 交换，即得到 $\exp G' = p = \exp Z(G)$，于是 $Z(G)$ 是初等交换 p-群.

(4) 由 $p \neq 2$, $c(G) \leq 2$ 和 $\exp G' \leq p$ 推知 G 为 p-交换群，即 G 中满足

$$(ab)^p = a^p b^p, \qquad \forall a, b \in G.$$

又因 $a^p \in \Phi(G)$, 它被任一 $h \in H$ 中心化，即 $[a^p, h] = 1$. 于是有

$$\begin{aligned}[a,h]^p &= (a^{-1}a^h)^p = a^{-p}(a^h)^p \\ &= a^{-p}(a^p)^h = [a^p, h] = 1.\end{aligned}$$

因为 G 是 p-交换的，由 $G = [G,H] = \langle [a,h] \mid a \in G, h \in H\rangle$ 的生成元均系 p 阶元，故得 $\exp G = p$. □

在定理 4.1 中出现的 p-群，即初等交换 p-群或满足 $Z(G) = G' = \Phi(G) = \Omega_1(Z(G))$ 的非交换 p-群，我们称之为*特殊 p-群*. 而如果非交换的特殊 p-群 G 又满足 $|Z(G)| = p$, 则称之为*超特殊 p-群*. 它们在有限单群的研究中十分有用. 超特殊 p-群的构造很容易确定. 事实上，它们是由若干个 p^3 阶非交换群所组成的中心积，欲知其详，可参看 D. Gorenstein 的 "*Finite Groups*" 中定理 5.5.2.

p-群 G 还有其他"小的"特征子群，借助于它们可以判断一个 p'-群在 G 上的作用是否平凡. 例如，Thompson 证明了下述定理:

定理 4.2 *任一 p-群 G 具有特征子群 C, 满足:*
(1) $c(C) \leq 2$ 且 $C/Z(C)$ 是初等交换 p-群;
(2) $[G,C] \leq Z(C)$;
(3) $C_G(C) \leq C$;
(4) G 的任一 p'-自同构 $\alpha \neq 1$ 在 C 上的作用非平凡.

这个定理下面用不到，我们就不证明了. 读者可参看 Gorenstein 的上述书中的定理 5.3.10.

最后，我们证明著名的 Blackburn 定理，它推广了前面的推论 2.8.

定理 4.3 设 p'-群 H 作用在 p-群 G 上，令

$$\Omega(G)=\begin{cases}\Omega_1(G), & p\neq 2,\\ \Omega_2(G), & p=2.\end{cases}$$

若 H 在 $\Omega(G)$ 上作用是平凡的，则它在 G 上的作用也是平凡的.

证 设 G 是使定理不真的极小阶反例. 因为对 G 的任一子群 K 有 $\Omega(K)\leq\Omega(G)$, 故由 G 的极小性， H 在 G 的每个 H-不变的真子群上作用是平凡的，但在 G 上作用非平凡，由定理 4.1 给出的 G 的结构说明 $\Omega(G)=G$, 与定理的假设矛盾. □

对于这个定理， T.J. Laffey 在下文中给出了一个不依赖于 Hall-Higman 简化定理的简短的新证明，但用到了 p-群的较深刻的结果. 可见

T.J. Laffey, A lemma on finite p-groups and some consequences, *Proc. Cambr. Phil. Soc.*, **75**(1974), 133-137.

习 题

1—5 题中都假定群 H 作用在群 G 上.

1. 设 $K\leq G$. 如果 H 在 K 上的作用平凡，则 H 在 $N_G(K)/C_G(K)$ 上作用亦平凡.

2. 设 $A\trianglelefteq H$. 则 $C_G(A)$ 是 G 的 H-不变子群.

3. 设 K 是 G 的 H-不变子群，则 $C_H(K)\trianglelefteq H$.

4. 设 H 在 $G-\{1\}$ 上作用是传递的，则 G 为初等交换 p-群.

5. 设 H 和 G 都是 p-群，则存在 G 的一个合成群列，使它的每一项都是 H-不变的.

6. p-群 H 不可约地作用在任意群 G 上. 则 $G\cong Z_p$, 或 $G\cong Z_{q^n}$ 对某个素数 q 和某个正整数 n 成立.

7. 设 π'-群 H 作用在 π-群 G 上. 令 $C=C_G(H)$. 则

(1) $N_G(C)=C_G(C)C$;

(2) 若 G 幂零，且 $C_G(C)\leq C$, 则 $C=G$.

8. 试如下给出 Thompson 引理 (引理 3.12) 的新证明：令 $D=G\rtimes B$, $W=C_G(B)\rtimes B$. 先证明 $C_D(W)\leq W$. 然后对于 $a\in A$, 作映射 $\varphi(a)$:

$xb \mapsto x^a b$, 其中 $x \in G$, $b \in B$. 证明 $\varphi(a)$ 是 D 的自同构, 这样 φ 使 A 作用在 D 上. 令 $U = C_D(A)$, 证明 $C_D(U) \le U$, 再用习题 7(2), 即得 $U = D$, 于是 $G \le U$.

9. (Glauberman) 设 π'-群 H 作用在 π-群 G 上, G 和 H 中至少有一个可解. 又设半直积 $S = G \rtimes H$ 作用在集合 Ω 上, 如果 G 在 Ω 上传递, 则 H 在 Ω 上必有不动点, 并且它的不动点集在 $C_G(H)$ 下是传递的.

10. 应用习题 9 给出引理 3.1 的一个新证明.

11. (1) 若 π'-群 H 作用在 π-群 G 上, 则在半直积 $S = G \rtimes H$ 中, 对任意的 $p \in \pi$, 成立 $\pi' \cup \{p\}$-Sylow 定理;

(2) 设 G 是 π-可分群, 则对任意的 $p \in \pi'$; G 中成立 $\pi \cup \{p\}$-Sylow 定理.

12. 设 G 是 π-群. $H \le \mathrm{Aut}(G)$, 又设 $U \le G$ 满足 $[G, H] \le U$ 且 $[U, H] = 1$ 则 H 是 π-群. 并举例说明 H 不一定等于 1.

13. p'-群 H 作用在 p-群 G 上.

(1) 若 $[G, H] = G$, 则 $C_G(H) \le \Phi(G)$;

(2) 若 $[G, H] \le \Phi(G)$, 则 $C_G(H) = G$.

14. π'-群 H 作用在 π-群 G 上. 设 $K \le C_G(H)$,$x \in G$ 满足 $K^x \le C_G(H)$, 则存在 $y \in C_G(H)$ 使 $K^x = K^y$.

15. 幂零群 H 作用在可解群 G 上, 若 $C_G(H) = 1$, 则对 G 的任一 H-不变正规子群 N, 有 $C_{G/N}(H) = 1$.

16. 设 G 是 p-可解群, $P \in \mathrm{Syl}_p(G)$,A 是 P 的极大交换正规子群, 则 G 的每个 A-不变 p'-子群 K 必在 $O_{p'}(G)$ 内.

17. 设非循环交换 p'-群 H 作用在 p-群 G 上, 则

$$G = \prod_{x \in H - \{1\}} C_G(x).$$

18. 若特殊 p-群 P 忠实且不可约地作用在 p'-群 G 上, 则 P 必为 Z_p 或超特殊 p-群.

19. 设 P 是 64 阶群, 且 $Z(P) = P'$ 是 Klein 四元群, 如果 P 有一 5 阶自同构, 证明 P 是特殊 2-群, 并且若不计同构被唯一地确定.

20. 设 P 是 2-群, A 是 P 的一个奇阶自同构群, 假定 A 在 P 的每个交换特征子群上作用是平凡的, 且 $[P, A] = P$. 则 P 必为非交换特殊 2-群.

第 VIII 章

转移， ZJ-定理和 p-幂零群

在第 II 章 §5 中，我们研究了转移映射的初步性质，并应用它们证明了 p-幂零群的一个充分条件 ——Burnside 定理. 在本章的前五节，我们将进一步研究转移映射的性质，证明几个较深刻的结果. 然后证明著名的 Glauberman ZJ-定理，并借助于 ZJ-定理，证明 Glauberman-Thompson p-幂零准则. 在本章的最后两节，我们将应用第 VII 章和本章前半的结果给出 Burnside p^aq^b-定理的一个群论证明，并证明著名的 Thompson 定理，它断言每个 Frobenius 群的 Frobenius 核是幂零群，而这曾是一个著名的、长达半个多世纪的猜想.

§1. Grün 定理

设 G 为有限群， $P \in \mathrm{Syl}_p(G)$. 本节我们进一步研究转移映射 $V_{G\to P}$, 并证明 Grün 的两个重要定理.

我们先给出如下的

定义 1.1 设 G 为有限群， p 为素数. 我们定义

(1) $O^p(G) = \langle g \in G \mid p \nmid o(g) \rangle$;

(2) $G'(p) = O^p(G)G'$.

显然 $O^p(G)$ 和 $G'(p)$ 都是 G 的特征子群. 它们具有如下的性质:

命题 1.2 (1) $G/O^p(G)$ 是 p-群， $G/G'(p)$ 是交换 p-群；

(2) 设 $N \trianglelefteq G$. 若 G/N 是 p-群，则 $O^p(G) \leq N$; 而若 G/N 为交换 p-群，则 $G'(p) \leq N$;

(3) 设 $P \in \mathrm{Syl}_p(G)$, 则 $G = O^p(G)P = G'(p)P$. 于是有

$$G/O^p(G) \cong P/P \cap O^p(G), \qquad G/G'(p) \cong P/P \cap G'(p). \quad (1.1)$$

证 (1) 对任一元 $x \in G$, 可找到 p 的适当方幂 p^i, 使 x^{p^i} 为一 p'-元，故 $x^{p^i} \in O^p(G)$, 这说明商群 $G/O^p(G)$ 全由 p-元组成，从而为 p-群. 因为 $O^p(G) \leq G'(p)$, $G/G'(p)$ 也是 p-群，又因为 $G' \leq G'(p)$, 故 $G/G'(p)$ 是交换 p-群.

(2) 设 x 是 G 的任一个 p'-元，则 x 在 p-群 $\overline{G} = G/N$ 中的像 $\bar{x} = \bar{1}$, 故 $x \in N$. 由此得到 $O^p(G) \leq N$. 若 $\overline{G} = G/N$ 为交换 p-群，则还应有 $G' \leq N$, 于是 $G'(p) = O^p(G)G' \leq N$.

(3) 因为 $G/O^p(G)$ 是 p-群，故 $|G|_{p'}$ 整除 $|O^p(G)|$, 从而 $|G| = |G|_{p'}|G|_p$ 整除 $|O^p(G)P|$, 故 $G = O^p(G)P$. 显然还成立 $G = G'(p)P$. 最后，根据第二同构定理，便得 (1.1) 式. □

在本节中的以下部分，我们将集中研究 $G'(p)$ 的性质，而对特征子群 $O^p(G)$, 我们将于以后各节加以讨论.

命题 1.3 设 G 为有限群， $P \in \mathrm{Syl}_p(G)$, 则

(1) $P \cap G'(p) = P \cap G'$;

(2) $V_{G\to P}(G) = V_{G\to P}(P) \cong P/P \cap G' \cong G/G'(p)$.

证 (1) 显然 $P \cap G' \leq P \cap G'(p)$. 以下证相反的包含关系. 由

$$G'(p)/G' = O^p(G)G'/G' = O^p(G/G'),$$

成立 $G/G' = G'(p)/G' \times PG'/G'$. 由此立得 $P \cap G'(p) \leq PG' \cap G'(p) \leq G'$.

(2) 将 $V_{G\to P}$ 简记为 V. 因为 V 是同态，而 $V(G)$ 是 p-群，故 G 的每个 p'-元 $x \in \mathrm{Ker}\ V$. 于是 $O^p(G) \leq \mathrm{Ker}\ V$. 又因为 $V(G)$ 是交换群，故有 $G' \leq \mathrm{Ker}\ V$. 这说明 $G'(p) \leq \mathrm{Ker}\ V$. 但 $G = G'(p)P$, 从而成立 $V(G) = V(G'(p)P) = V(P)$.

为完成证明, 还须证 $V(P)\cong P/P\cap G'$. 为此只须证 $\text{Ker } V|_P = P\cap G'$. 记 $K=\text{Ker } V|_P$, $P^*=P\cap G'$. 显然有 $P^*\le K$. 设 $g\in P$, 则根据 II.§5 中的 (5.1) 式, 并采用相应的记法, 便得

$$V(g)=\prod_i x_i g^{f_i} x_i^{-1} P' = \prod_i g^{f_i}[g^{f_i}, x_i^{-1}]P' = g^n c P',$$

其中 $n=|G:P|, c\in P^*$.

由于 $(n,p)=1$, 故若 $g\notin P^*$, 则 $g^n\notin P^*$ 从而有 $V(g)\notin P^*/P'$. 这表明 $|V(P)|\ge |P/P^*|$, 即 $|P/K|\ge |P/P^*|$, 由此即得 $K=P^*$. □

由命题 1.3 的证明可以直接得到以下结果, 其证明留给读者.

命题 1.4 设 G 为有限群, $P\in \text{Syl}_p(G)$, 则

$$P\cap G' = \langle [x,s]\in P \mid x\in P, s\in G\rangle.$$

定理 1.5 (Grün 第一定理) 设 G 是有限群, $P\in \text{Syl}_p(G)$. 则

$$P\cap G' = \langle P\cap N_G(P)', P\cap P'^g \mid g\in G\rangle.$$

证 令 $D=\langle P\cap N_G(P)', P\cap P'^g | g\in G\rangle$. 显然 $P'\le D\le P\cap G'$, 从而有 $D\trianglelefteq P$

设 $D<P\cap G'$. 在 $(P\cap G')\setminus D$ 中取一最小阶元素 u, 我们来计算 $V_{G\to P}(u)$.

首先考虑 G 的双陪集分解 $G=\bigcup_i Pg_iP$.

由于 $u\in P$, 则通过 u 右乘将把每个双陪集变到自身, 从而导出该双陪集中所含诸右陪集的一个置换, 下面我们仔细分析这些置换.

我们固定一个双陪集 PgP. 设由 u 右乘所得到的右陪集的置换为 $\tilde{u}$, 并且假设 $\tilde{u}$ 的轮换分解为

$$\tilde{u}=\prod_{i=1}^{r}\left(Pgx_i,\ Pgx_iu,\ \cdots,\ Pgx_iu^{p^{m_i}-1}\right),$$

其中 $x_1,\cdots,x_r\in P$. 显然 $\sum_i p^{m_i}=|PgP:P|=p^s$, $s\geq 0$. 我们还不妨设 $m_1\leq\cdots\leq m_r$. 并通过适当选择双陪集代表元 g 可令 $x_1=1$, 即在 (1.1) 式中把最短轮换放在最前面, 并且它包含右陪集 Pg. 这时我们有 $Pgx_iu^{p^{m_i}}=Pgx_i$, 于是有 $t_i=gx_iu^{p^{m_i}}x_i^{-1}g^{-1}\in P$, 特别地, 有 $gu^{p^{m_1}}g^{-1}\in P$. 为计算 $V_{G\to P}(u)$, 我们还需计算 $\prod_i t_i$. 为此, 我们分别讨论下列两种情形.

情形 1. $s\geq 1$. 我们将证明 $\prod_i t_i\in D$.

首先我们有 $d_i=gu^{-p^{m_i}}g^{-1}t_i=g[u^{p^{m_i}};x_i^{-1}]g^{-1}\in P'^{g^{-1}}$.

又由 $gu^{p^{m_1}}g^{-1}\in P$ 及 $m_i\geq m_1$ 有 $gu^{p^{m_i}}g^{-1}\in P$. 故 $d_i=gu^{-p^{m_i}}g^{-1}t_i=(gu^{p^{m_i}}g^{-1})^{-1}t_i\in P$, 故 $d_i\in P\cap P'^{g^{-1}}\leq D$, 而因为 $t_i=gu^{p^{m_i}}g^{-1}d_i$, 故 $\prod_i t_iD=\prod_i(gu^{p^{m_i}}g^{-1})\prod_i d_iD=gu^{p^s}g^{-1}D$. 由于 $gu^{p^{m_1}}g^{-1}\in P$, 故 $gu^{p^s}g^{-1}\in P$. 又由于 $u\in G'$, 有 $gu^{p^s}g^{-1}\in G'$. 于是 $gu^{p^s}g^{-1}\in P\cap G'$. 最后, 由于 $s\geq 1$, 故 $o(gu^{p^s}g^{-1})<o(u)$, 则由 u 的选择有 $gu^{p^s}g^{-1}\in D$. 从而有 $\prod_i t_i\in D$.

情形 2. $s=0$.

这时 $PgP=Pg$, 只含一个右陪集. 因此 $g\in N_G(P)$, $\prod_i t_i=t_1=gug^{-1}=u[u,g^{-1}]$, 其中 $[u,g^{-1}]\in P\cap N_G(P)'\leq D$.

根据以上讨论, 并由 $V_{G\to P}(u)$ 之定义, 即得 $V(u)=u^kdP'$, 其中 $k=|N_G(P):P|, d\in D$. 又因为 $u\in P\cap G'\leq \mathrm{Ker}\,V$, 故有 $V(u)=P'$, 从而成立 $u^kd\in P'\leq D$. 这推出 $u^k\in D$. 但这时 $(p,k)=1$, 故 u 为 p-元, 从而得 $u\in D$, 与 $u\notin D$ 相矛盾. □

为了叙述 Grün 第二定理, 我们还需以下

定义 1.6 设 G 是有限群, $P\in \mathrm{Syl}_p(G)$, 我们称 G 是 p-正规的, 如果对任意 $g\in G$ 有

$$Z(P)^g\leq P\Longrightarrow Z(P)^g=Z(P). \tag{1.1}$$

注意 p-正规的概念不依赖于 p-Sylow 子群的特殊选择. 设 G 为 p-正规, 且对于 $P\in\mathrm{Syl}_p(G)$, 定义 1.6 中条件 (1.1) 成立. 设 $P_1\in\mathrm{Syl}_p(G)$, 并假定 $Z(P_1)^g\leq P_1$, 以下证明 $Z(P_1)^g=Z(P_1)$. 由 Sylow 定理, 存在 $x\in G$, 使得 $P_1=P^x$, 于是有 $Z(P^x)^g\leq P^x$, 即

$Z(P)^{xgx^{-1}} \le D$. 由于 G 为 p-正规，则有 $Z(P) = Z(P)^{xgx^{-1}}$，从而有 $Z(P^x)^g = Z(P) = Z(P^x)$，即 $Z(P_1)^g = Z(P_1)$.

显然我们有

命题 1.7 设 G 是有限群，$P \in \mathrm{Syl}_p(G)$.
(1) 若 P 交换，则 G 为 p-正规；
(2) 若 G 的任意二 Sylow 子群交为 1, 则 G 为 p-正规.

(证明从略.)

定理 1.8 (Grün 第二定理). 设 G 是 p-正规的有限群，$P \in \mathrm{Syl}_p(G)$, 且 $N = N_G(Z(P))$, 则成立 $G/G'(p) \cong N/N'(p)$.

证　由于 $Z(P)$ char P, 故 $P \le N$, 特别地，$P \in \mathrm{Syl}_p(N)$. 根据命题 1.3 有 $G/G'(p) \cong P/P \cap G'$, $N/N'(p) \cong P/P \cap N'$. 于是仅需证明 $P \cap G' = P \cap N'$.

显然 $P \cap N' \le P \cap G'$, 为证明相反的包含关系，我们应用定理 1.4, 即 $P \cap G' = \langle P \cap N_G(P)', P \cap P'^g | g \in G \rangle$.

设 $T = P \cap P'^g$, 我们证明 $T \le P \cap N'$. 显然 $Z(P) \le N_G(T)$. 又因 $Z(P)^g$ 是 P^g 的中心，故 $Z(P)^g \le N_G(T)$. 于是存在 $N_G(T)$ 的两个 Sylow p-子群 P_1, P_2 使 $Z(P) \le P_1$, $Z(P)^g \le P_2$, 根据 Sylow 定理，存在 $s \in N_G(T)$, 使 $P_1 = P_2^s$. 再取 G 的 Sylow p-子群 $P^* \ge P_1$. 则有 $Z(P) \le P_1 \le P^*$, $Z(P)^{gs} \le P_2^s = P_1 \le P^*$.

由 G 的 p-正规性，有 $Z(P) = Z(P)^{gs}$, 即 $gs \in N$. 又因 $s \in N_G(T)$, 故 $T = T^s = P^s \cap P'^{gs}$. 由于 $P \le N$, 故 $P'^{gs} \le N'^{gs} = N'$, 于是 $T \le N'$. 又因 $T \le P$, 故 $T \le P \cap N'$,

又因 $Z(P)$ char P, 故 $N_G(P) \le N$, 从而有 $P \cap N_G(P)' \le P \cap N'$. 这样我们就证明了 $P \cap G' = P \cap N'$. □

§2. p-幂零群

首先我们复述一下 p-幂零群的定义.

定义 2.1 我们说有限群 G 是 p-幂零的，如果 $p \nmid |O^p(G)|$.

这时 $O^p(G)$ 就是 G 的正规 p-补. 对于任一 $P\in \mathrm{Syl}_p(G)$, 都有 $P\cap O^p(G)=1$. 由定义 2.1 还可看出, 若 G 为 p-幂零, 则 $O^p(G)$ 恰由 G 中所有 p'-元组成.

命题 2.2 若 G 是 p-幂零群, 则 G 的每个子群和商群也都是 p-幂零群.

证 (1) 设 $H\leq G$. 因为 $O^p(G)$ 恰包含 G 中所有 p-元, 于是 H 的子群 $H\cap O^p(G)$ 也恰包含 H 中所有的 p'-元, 即 $H\cap O^p(G)=O^p(H)$. 因此 H 为 p-幂零群.

(2) $N\trianglelefteq G$, $\overline{G}=G/N$. 令 $\overline{K}=O^p(G)N/N$. 由 G 的 p-幂零性, $O^p(G)$ 全由 p'-元组成, 故 $\overline{K}$ 也全由 p'-元组成. 又因 $\overline{G}/\overline{K}\cong G/O^p(G)N$ 是 p-群, 故 $O^p(\overline{G})=\overline{K}$, 即 $\overline{G}$ 也是 p-幂零群. □

下面给出 p-幂零群的一个刻划, 它对应于幂零群用中心群列的刻划. 为此先证明一个引理.

引理 2.3 设 G 是 p-幂零群, N 是 G 的极小正规子群, 且 $p\mid |N|$, 则 $N\leq Z(G)$, 且 $|N|=p$.

证 由于 G 为 p-幂零群, $O^p(G)$ 是 p'-群, 于是 $O^p(G)\cap N$ 是 p'-群. 但由 $p\mid |N|$ 及 N 的极小性, 必有 $O^p(G)\cap N=1$. 因此 $|N|=|N/O^p(G)\cap N|=|O^p(G)N/O^p(G)|$ 等于 p 的方幂, 故 N 是 p-群.

另外, 由 $O^p(G)\cap N=1$, 推知 N 与 $O^p(G)$ 元素间可交换. 任取 $P\in \mathrm{Syl}_p(G)$, 显然有 $N\leq O_p(G)\leq P$. 我们断言必有 $N\leq Z(P)$. 若否, 则有 $1\neq N_1=N\cap Z(P)\trianglelefteq P$, 且 $N_1\lneqq N$. 由 $N_1\leq Z(P)$ 及 N_1 与 $O^p(G)$ 元素可交换, 故 $N_1\leq Z(G)$, 特别地, $N_1\trianglelefteq G$, 这与 N 的极小性相矛盾. 从而, $N\leq Z(G)$. 进一步, N 的任何 p 阶子群都是 G 的正规子群, 故由 N 的极小性可知 $|N|=p$. □

定理 2.4 下列命题等价:

(1) G 是 p-幂零群;

(2) 设

$$1 = G_0 < G_1 < \cdots < G_r = G \tag{2.1}$$

是 G 的任一主群列. 若 $p \mid |G_i/G_{i-1}|$, 则 $G_i/G_{i-1} \le Z(G/G_{i-1})$;

(3) 存在 G 的主群列 (2.1), 使对任一 i, 或者 $p \nmid |G_i/G_{i-1}|$, 或者 $G_i/G_{i-1} \le Z(G/G_{i-1})$.

证 (1) $\Rightarrow$ (2): 由命题 2.2 和引理 2.3 得到

(2) $\Rightarrow$ (3): 显然.

(3) $\Rightarrow$ (1): 用对 $|G|$ 的归纳法. 因为 G/G_1 亦满足条件 (3), 于是 G/G_1 是 p-幂零群. 设 K/G_1 是 G/G_1 的正规 p-补, 若 $p \nmid |G_1|$, 则 K 为 G 的正规 p-补, 于是 G 为 p-幂零. 而若 $p \mid |G_1|$, 则由 (3) 中条件有 $G_1 \le Z(G)$, 因此必然有 $|G_1| = p$. 在 K 中应用 Schur-Zassenhaus 定理, 存在 G_1 的补群 K_1, 且有 $K = K_1 \times G_1$. 于是 $K_1 \text{ char } K \trianglelefteq G$, 从而 $K_1 \trianglelefteq G$, 且 $|K_1| = |K/G_1| = |G/G_1|_{p'} = |G|_{p'}$, 故 K_1 是 G 的正规 p-补. □

最后证明 p-幂零群的一个必要条件.

定理 2.5 设有限群 G p-幂零, 则 G 必为 p-正规.

证 设 $K = O^p(G)$, $P \in \mathrm{Syl}_p(G)$. 则因 $G/K \cong P$, 有 $Z(G/K) = Z(P)K/K$. 于是对任意的 $g \in G$, 有

$$Z(P)K = (Z(P)K)^g = Z(P)^g K.$$

若 $Z(P)^g \le P$, 则 $Z(P)^g = Z(P)^g K \cap P = Z(P)K \cap P = Z(P)(K \cap P) = Z(P)$, 故 G 为 p-正规的. □

§3. 极小非 p-幂零群

为了进一步研究有限群的 p-幂零性, 我们来考察极小非 p-幂零群的性质. 首先证明 Burnside 的一个引理.

引理 3.1 设 P, P_1 是 G 的两个 Sylow p-子群, 且子群 $1 \neq M \trianglelefteq P$, $M < P_1$, 但 $M \ntrianglelefteq P_1$. 则存在 $x \in G$ 使 $o(x) = q^b$, 其中 q 为素数, $q \neq p$, 并满足

(1) $x \notin N_G(M)$,

(2) $J = \langle M, M^x, \cdots, M^{x^{q^b-1}} \rangle$ 是 p-群,

(3) $x \in N_G(J) \setminus C_G(J)$.

证 在 G 的 Sylow p-子群中选择满足如下条件的一个群 (不妨仍叫做 P_1):

(i) $M < P_1$,

(ii) $M \ntrianglelefteq P_1$,

(iii) $|N_{P_1}(M)|$ 尽可能大.

令 $S = N_{P_1}(M)$, 当然有 $S < P_1$. 因为 P, $S \leq N_G(M)$, 必存在 $y \in N_G(M)$, 使 $P^y \geq S$. 若以 P^y 代替 P, 则不妨假设 $P \geq S$.

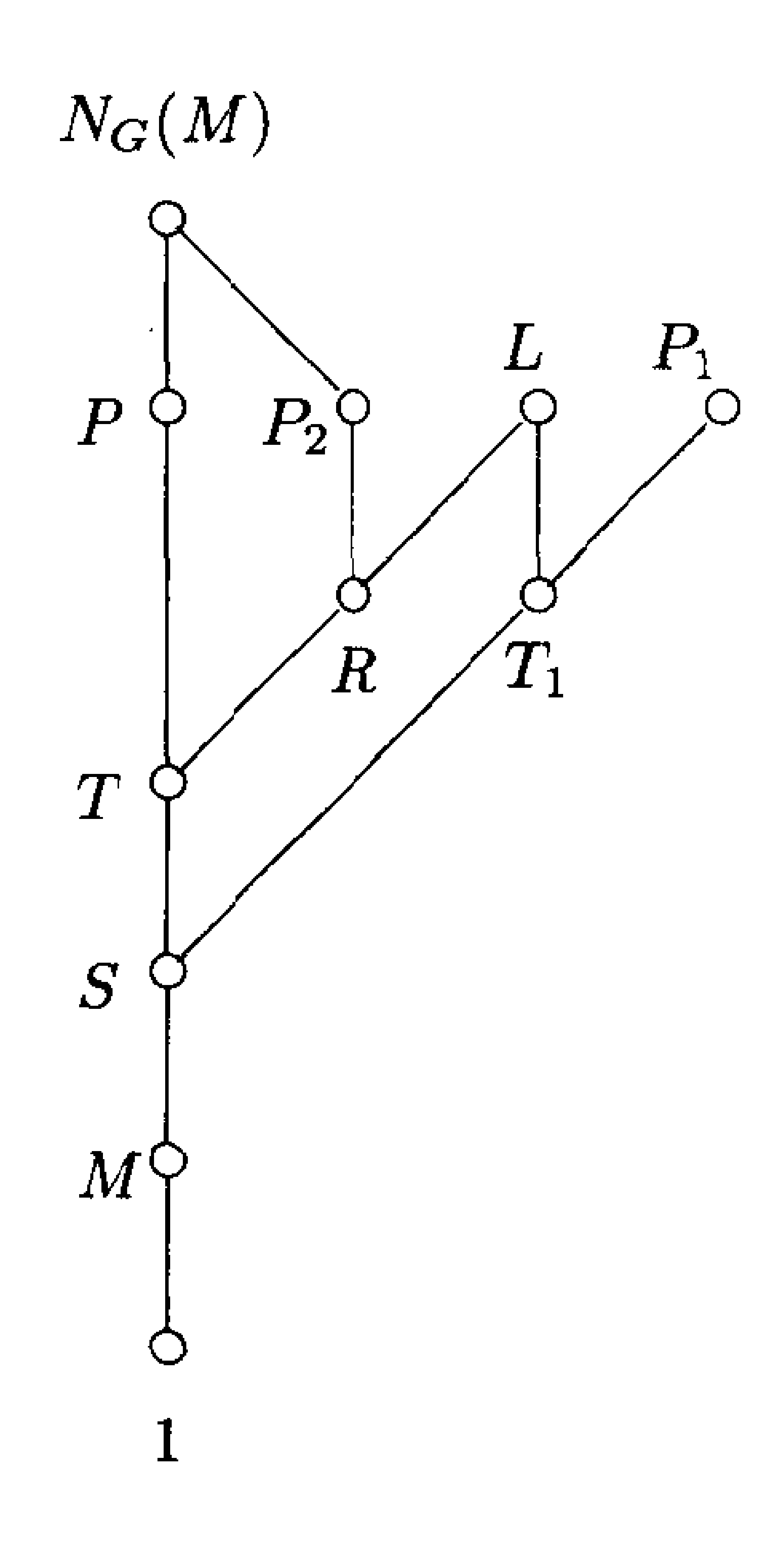


图 3.1

令 $T = N_P(S)$, $T_1 = N_{P_1}(S)$. 因 $|S| < |P_1|$, 故 $T > S, T_1 > S$, 从而 $M \ntrianglelefteq T_1$. 这时有 $S \trianglelefteq \langle T, T_1 \rangle = L$, 但 $M \ntrianglelefteq L$.

在 L 中取一包含 T 的 Sylow p-子群 R, 并设 $P_2 \geq R$, $P_2 \in \mathrm{Syl}_p(G)$. 因为 $N_{P_2}(M) \geq N_R(M) \geq T \geq S$, 故由 P_1 的选择, 必有 $M \trianglelefteq P_2$, 从而 $M \trianglelefteq R$. (以上诸子群间的关系请参看图 3.1).

假如 L 中所有阶为异于 p 的素数方幂的元皆正规化 M, 则这些元素生成的子群, 即 $O^p(L)$, 必正规化 M. 但又有 R 正规化 M, 而 $L = O^p(L)R$, 故 $M \trianglelefteq L$, 矛盾. 因此必有一元素 $x \in L$, $o(x) = q^b$,

$q \neq p$, 使得 $M^x \neq M$. 考虑子群 M^{x^i}, $i = 0, 1, \cdots, q^b - 1$. 因为 $M \lhd S \lhd L$, 有 $M^{x^i} \lhd S^{x^i} = S$. 于是 $J = \langle M, M^x, \cdots, M^{x^{q^b-1}} \rangle \leq S$, 因而 J 为 p-群. 显然 $J^x = J$. 但因 $M^x \neq M$, 故 $x \notin C_G(J)$, 因此 $x \in N_G(J) \setminus C_G(J)$. □

为了揭示极小非 p-幂零群之结构，我们还需如下两个引理.

引理 3.2 *设 $P \in \mathrm{Syl}_p(G)$, U char P, 且对某个 $g \in G$, 成立 $U^g \trianglelefteq P$, 则有 $U = U^g$.*

证 因为 U char P, $U^g \leq P$, 故 P 和 $P^{g^{-1}}$ 是 $N_G(U)$ 中二个 Sylow p-子群. 故有 $h \in N_G(U)$ 能使 $P^h = P^{g^{-1}}$, 于是 $hg \in N_G(P)$. 又由 U char P, 有 $N_G(P) \leq N_G(U)$. 于是 $hg \in N_G(U), g \in N_G(U)$. 这就得到 $U = U^g$. □

引理 3.3 *设有限群 G 非 p-正规，则存在 G 的一个 p-子群 J 和元素 $x \in G$, 使得 $x \in N_G(J) \setminus C_G(J)$, 且 $o(x) = q^b$, 其中 $q \neq p$ 是素数.*

证 设 $P \in \mathrm{Syl}_p(G)$, 因为 G 非 p-正规，则存在 $g \in G$ 使 $Z(P)^g \leq P$, 但 $Z(P)^g \neq Z(P)$. 于是由引理 3.2, 必有 $Z(P)^g \ntrianglelefteq P$. 取 $M = Z(P)$, $P_1 = P^{g^{-1}}$, 由引理 3.1 即得结论. □

以下定理揭示了极小非 p-幂零群之构造.

定理 3.4 (Itô) *设有限群 G 的每个真子群均 p-幂零. 但 G 非 p-幂零，则*

(1) G 的每个真子群幂零;

(2) $|G| = p^a q^b$, 其中 q, p 为素数且 $q \neq p$, a, b 均为正整数;

(3) G 的 Sylow p-子群 $P \trianglelefteq G$, 且若 $p \neq 2$, 则 $\exp P = p$, 而对于 $p = 2$, 有 $\exp P \leq 4$;

(4) G 的 Sylow q-子群循环.

证 设 $P \in \mathrm{Syl}_p(G)$. 首先证明 $P \trianglelefteq G$. 为此分下列两种情况进行讨论.

首先设 G 非 p-正规, 则由引理 3.3, 存在 G 的 p-子群 J 和元素 $x \in N_G(J) \setminus C_G(J)$, $o(x) = q^b$, $q \neq p$. 如果 $J\langle x\rangle < G$, 则由定理条件知 $J\langle x\rangle$ 为 p-幂零, 于是 $J\langle x\rangle = J \times \langle x\rangle$, 即 $x \in C_G(J)$, 矛盾. 故必有 $J\langle x\rangle = G$, 且 $P = J \trianglelefteq G$.

再设 G 为 p-正规, 若 $N = N_G(Z(P)) < G$, 则由定理假设, N 为 p-幂零, 于是有 $N/N'(p) \neq 1$. 根据 Grün 第二定理, $G/G'(p) \cong N/N'(p)$, 故得 $G'(p) < G$. 由定理假设, $G'(p)$ 是 p-幂零群. 因为 $G'(p) \geq O^p(G)$, 故 $O^p(G)$ 是 $G'(p)$ 的正规 p-补, 因而也是 G 的正规 p-补, 这便得到 G 的 p-幂零性, 与假设矛盾. 故必有 $N_G(Z(P)) = G$. 如果 $Z(P) = P$, 就得到 $P \trianglelefteq G$, 而如果 $Z(P) < P$, 考虑 $\overline{G} = G/Z(P)$. 假定 $\overline{G}$ 非 p-幂零, 应用归纳假定当有 $P/Z(P) \trianglelefteq \overline{G}$, 从而 $P \trianglelefteq G$. 而若 $\overline{G}$ p-幂零, 并设 $M/Z(P)$ 是 $\overline{G}$ 的正规 p-补, 则由 $p \mid |\overline{G}|$, 故 $M < G$, 于是 M p-幂零. 但 M 的正规 p-补即是 G 的正规 p-补, 故 G 亦 p-幂零, 矛盾. 由此矛盾即得 $P \trianglelefteq G$.

其次再来证明, G 的每个真子群为幂零群. 由 $P \trianglelefteq G$, 根据 Schur-Zassenhaus 定理, G 中存在 p-补群 Q. 由于 G 非 p-幂零, 故 $Q \not\leq C_G(P)$. 因此可找到 $x \in Q \setminus C_G(P)$, $o(x) = q^b$, $q \neq p$. 这时 $P\langle x\rangle$ 必然也非 p-幂零, 故有 $G = P\langle x\rangle$, 特别地, 有 $|G| = p^a q^b$, G 是 q-幂零的. 若 $H < G$, 则 H 既为 p-幂零群又为 q-幂零群. 故 H 为幂零群. 至此已证得 (1), (2) 和 (4). 而 (3) 则可由 IV, 定理 4.2 得到. □

最后, 我们应用定理 3.4 证明著名的 Frobenius 定理.

定理 3.5 (Frobenius) 设 G 为有限群, 则下列陈述等价:

(1) G 是 p-幂零的;

(2) 对 G 的任一 p-子群 $U \neq 1$, $N_G(U)/C_G(U)$ 是 p-群;

(3) 对 G 的任一 p-子群 $U \neq 1$, $N_G(U)$ 为 p-幂零.

证 (1)⇒(3): 由命题 2.2 立得;

(3)⇒(2): 设 K 是 $N = N_G(U)$ 正规 p-补, 则由 $K \trianglelefteq N, U \trianglelefteq N$, 有 $KU = K \times U$. 于是 $K \leq C_G(U)$, 故 $N_G(U)/C_G(U)$ 是 p-群.

(2)⇒(1): 设 G 是使结论不真的最小反例. 对 G 的任一真子群 H, 设 U 是 H 的 p-子群, 则由 $N_H(U)/C_H(U) = N_G(U) \cap H/C_G(U) \cap H \cong (N_G(U) \cap H)C_G(U)/C_G(U) \le N_G(U)/C_G(U)$ 知 $N_H(U)/C_H(U)$ 也是 p-群. 再由 G 的极小性知 H 为 p-幂零. 因 G 适合定理 3.4 之条件, 故由该定理可知 G 的 p-Sylow 子群 $P \trianglelefteq G$. 于是由 $N_G(P)/C_G(P) = G/C_G(P)$ 是 p-群, 有 $G = P \cdot C_G(P)$, 且 $O^p(G) \le C_G(P)$. 若 $C_G(P) < G$, 则由定理假设, $C_G(P)$ 是 p-幂零的, 于是 $O^p(G)$ 是 $C_G(P)$ 的正规 p-补, 同时也是 G 的正规 p-补, 于是 G 为 p-幂零. 而若 $C_G(P) = G$, 则由 Schur-Zassenhaus 定理, P 在 G 中的补群 K 必满足 $P \times K = G$, 于是 $K \trianglelefteq G$, 这就证明了 G 为 p-幂零. □

§4. Glauberman ZJ-定理

ZJ-定理是有限群理论中的一个十分重要和著名的定理. 它可以看作是以上所讲的 p-幂零准则的一种推广. 这一定理有许多重要应用, 特别是利用这一定理可以证明 Glauberman-Thompson p-幂零准则 (见 §5).

为了叙述和证明 ZJ-定理, 我们先给出如下定义.

定义 4.1 设 G 为一有限群.

(1) 我们说 G 是 **p-约束的**, 如果对于 $P \in \mathrm{Syl}_p(O_{p',p}(G))$, 成立 $C_G(P) \le O_{p',p}(G)$;

(2) 设 p 是一个奇素数, $O_p(G) \ne 1$. 我们说 G 是 **p-稳定的**, 若下列条件成立:

令 P 为 G 的 p-子群, 能使 $O_{p'}(G)P \trianglelefteq G$. A 为 $N_G(P)$ 的 p-子群, 能使 $[P, A, A] = 1$, 则必然成立:

$$AC_G(P)/C_G(P) \le O_p(N_G(P)/C_G(P)).$$

对于 p-稳定性, 我们不加证明地给出下面的定理.

定理 4.2 *令 G 为有限群, p 是奇素数. 如果 G 中任一截断都不同构于 $SL(2,p)$, 则 G 是 p-稳定的.*

(证明可见 D. Gorenstain 的书 "Finite Groups" 第三章 §8 和第六章 §5.)

作为定理 4.2 的推论，我们有

推论 4.3 设 G 是有限 p-可解群，$p \geq 5$ 或当 $p=3$ 时 G 中任一截断都不同构于 $SL(2,3)$, 则 G 是 p-稳定的.

(证明可见 D. Gorenstain 的书 "Finite Groups" 第六章 §5.)

以上两个结论在下节中将要引用.

定理 4.4 令 G 为有限群，且 G 既是 p-约束又是 p-稳定的. 设 $P \in \mathrm{Syl}_p(G)$, A 为 P 的交换正规子群，则 $A \leq O_{p',p}(G)$.

证 令 $Q = P \cap O_{p',p}(G)$, 则 $O_{p'}(G)Q \trianglelefteq G$, 又由假定 $A \leq N_G(Q)$ 且 $[Q,A,A]=1$, 则由 G 是 p-稳定的便有

$$AC_G(Q)/C_G(Q) \leq O_p(N_G(Q)/C_G(Q)).$$

又因 G 为 p-约束的, 立得 $C_G(Q) \leq O_{p',p}(G) = O_{p'}(G)Q$. 由于 $Q \in \mathrm{Syl}_p(O_{p',p}(G))$, 便有 $G = O_{p'}(G)N_G(Q)$. 若令 $\overline{G} = G/O_{p'}(G)$, 则 $N_G(Q)$ 映到 $\overline{G}$ 上，由此便有 $\overline{AQ}/\overline{Q} \leq O_p(\overline{G}/\overline{Q})$. 但由 $\overline{Q} = O_p(\overline{G})$, $O_p(\overline{G}/\overline{Q}) = 1$, 便有 $\overline{AQ} \leq \overline{Q}$, 故 $\overline{A} \leq \overline{Q}$, 即 $A \leq O_{p',p}(G)$. □

上述定理在应用时，往往采取下列较为一般的形式.

推论 4.5 令 G 为一群，p 为奇素数，$P \in \mathrm{Syl}_p(G)$, Q 为 P 的非平凡子群. 假定 $N = N_G(Q)$ 为 p-约束且是 p-稳定的，而 Q 为 $O_{p',p}(N)$ 的 Sylow p-子群. 则 Q 包含 P 的每一交换正规子群.

做为练习，请读者自行给出 4.5 的证明.

下面，我们再引入 p-群的 Thompson 子群的概念.

定义 4.6 令 P 为一 p-群. 令 $A(P)$ 为 P 的具有极大阶的交换子群之集合. 我们定义:

$$J(P) = \langle A \mid A \in A(P) \rangle,$$

$J(P)$ 叫做 P 的 Thompson 子群. 显然 $J(P)$ char P. Thompson 子群具有下列简单性质. 这些性质在本节和后面的一些章节中都要用到. 其证明十分简单，所以略去了.

引理 4.7 令 $P \in \mathrm{Syl}_p(G)$, 则有

(1) 若 R 为 P 的子群, 且其中包含 $A(P)$ 的一个元, 则 $A(R) \subseteq A(P)$, $J(R) \leq J(P)$;

(2) 若 $J(P) \leq Q \in \mathrm{Syl}_p(G)$, 则 $J(Q) = J(P)$;

(3) 若 $Q = P^x$, $x \in G$, 则 $J(Q) = J(P)^x$;

(4) 若有 $J(P) \leq R \leq G$, 且 R 为 p-群，则有 $J(P)$ char R.

Glauberman 定理的证明还依赖于集合 $A(P)$ 的某些性质.

引理 4.8 令 $A \in A(P)$, $B \leq P$, 则:

(1) $A = C_P(A)$, 特别地 $Z(P) \leq A$;

(2) B 正规化 $A \iff [B, A, A] = 1$

证 (1) 令 $x \in C_p(A)$, 则因 A 交换，故 $\langle x, A\rangle$ 也交换，再由 A 极大，便得 $x \in A$.

(2) 若 B 正规化 A, 则 $[B, A] \leq A$, 从而 $[B, A]$ 中心化 A. 反之，若 $[B, A, A] = 1$, 则 $[B, A] \leq C_G(A)$, 由 (1), 必有 $[B, A] \leq A$, 这表明 B 正规化 A. □

定理 4.9 (Thompson) 令 $A \in A(P)$, 并假定 $M = [x, A]$ 交换, $x \in P$, 则 $MC_A(M) \in A(P)$.

证 令 $C = C_A(M)$. 显然 MC 交换，因此仅需证明 $|MC| \geq |A|$, 便有 $MC \in A(P)$. 由于 $A = C_P(A)$ 且 M 交换, 故 $C \cap M = A \cap M = C_M(A)$. 从而有 $|MC| = |M||C|/|C \cap M| = |M||C|/|C_M(A)|$. 因此，要证 $|A| \leq |MC|$, 仅需证 $|M/C_M(A)| \geq |A/C_A(M)|$, 而为此又仅需证明，只要 $u, v \in A$ 分别属于 $C_A(M)$ 在 A 中的不同的陪集，则 $[x, u]$ 和 $[x, v]$ 分别属于 $C_M(A)$ 的不同的陪集.

假定有 $u, v \in A$ 能使 $[x, u]C_M(A) = [x, v]C_M(A)$, 则 $y = [x, u]^{-1}[x, v] \in C_M(A)$. 易知 $y = (x^u)^{-1}x^v$. 故有 $y = y^{u^{-1}} =$

$x^{-1}x^{vu^{-1}} = [x, vu^{-1}]$, 从而 $[x, vu^{-1}, a] = [y, a] = 1$, $\forall a \in A$. 又因 A 交换, $[vu^{-1}, a, x] = 1$. 由三子群引理及 $[x, A]$ 之交换性, 便可得 $[x, a, vu^{-1}] = 1$, $\forall a \in A$, 即有 $[M, vu^{-1}] = 1$, 从而 $vu^{-1} \in C_A(M)$. 这就证明了所需结论. □

定理 4.10 (Thompson 替换定理) 令 $A \in \mathcal{A}(P)$, 并令 B 为 P 的交换子群. 假定 A 正规化 B, 但 B 不正规化 A. 则可找到 $A^* \in \mathcal{A}(P)$ 具有如下性质:

(1) $A \cap B \lneqq A^* \cap B$;

(2) A^* 正规化 A.

证 AB 为一群且 $B \trianglelefteq AB$. 因 B 交换, 故 $N = N_B(A) \trianglelefteq AB$. 又因 B 不正规化 A, 故 $N < B$. 由于 $B/N \trianglelefteq AB/N$, 故 $B/N \cap Z(AB/N) \neq 1$, 则有 $x \in B \setminus N$, 其像包含在 $Z(AB/N)$ 之中. 故 $[x, A] \leq N \leq B$. 令 $M = [x, A]$, 则 M 交换. 由 4.9, $A^* = MC_A(M) \in \mathcal{A}(P)$. A^* 便满足条件 (1), (2).

由于 $M \leq N_B(A)$, 又 $C_A(M) \leq A$, 故 A^* 正规化 A. 进而, 因 $A \cap B$ 既中心化 x 又中心化 A, 故 $A \cap B \leq A^* \cap B$. 另一方面, 因 $x \notin N$, 故 $M = [x, A] \nleq A$, 但 $M \leq N \leq B$, 故 $A^* \geq M(A \cap B) > A \cap B$, 证完. □

下面我们证明 Glauberman 替换定理. 为此先证一个引理, 这一引理的证明过程中极其巧妙地运用了换位子的技巧.

引理 4.11 令 B 为一奇数阶群, A 交换且作用在 B 上, 还成立 $[B, B, A] = 1$. 则对任意的 $x \in B$, 由 $[x, A, A, A] = 1$ 便得 $[x, A]$ 交换.

证 假定 $[x, A, A, A] = 1$, 其中 $x \in B$, 今证明 $[x, a]$ 与 $[x, b]$ 交换, $\forall a, b \in A$.

由 Witt 公式, $[x, a, b]^{a^{-1}}[a^{-1}, b^{-1}, x]^b[b, x^{-1}, a^{-1}]^x = 1$. 因 A 交换, 故第二个换位子为 1. 又 $[x, A, A, A] = 1$ 表明第一个换位子与 a 交换, 故有 $[x, a, b] = ([b, x^{-1}, a^{-1}]^{-1})^x$. 由 IV, 命题 1.2(3) 以及 $[x, A, A, A] = 1$, 又有 $[x, a, b] = ([b, x^{-1}, a]^{a^{-1}})^x = [b, x^{-1}, a]^x$. 今

$[b,x^{-1}]=[x,b]^{x^{-1}}\in[x,b]B'$. 因 $[A,B']=1$, 则 $[b,x^{-1},a]=[x,b,a]$. 从而有 $[x,a,b]=[x,b,a]^x$. 通过归纳得

$$[x,b,a]^{x^n}=\begin{cases}[x,b,a], & n\text{为偶数},\\ [x,a,b], & n\text{为奇数}.\end{cases}$$

但 $o(x)\equiv 1(\mathrm{mod}\ 2)$, 故 $[x,a,b]=[x,b,a]$.

因 $[x,ab]=[x,a][x,b][x,b,a]=[x,b][x,a][x,a,b]$, 从而有 $[x,a][x,b]=[x,b][x,a]$. □

定理 4.12 (Glauberman 替换定理). *令 p-为奇素数, P 为一 p-群, $B\leq P$, 且 $B'\leq Z(J(P))$, 令 $A\in\mathcal{A}(P)$, 且 A 正规化 B, 但 B 不正规化 A, 则有 $A^*\in\mathcal{A}(P)$, 能使*

(1) $A\cap B\lneqq A^*\cap B$;

(2) A^* 正规化 A.

证 因 B 不正规化 A, 则 $[B,A]\nleq A=C_P(A)$, 从而 $[B,A,A]\neq 1$, 定义 $[B,A;1]=[B,A]$, 又归纳地定义 $[B,A;n]=[[B,A;n-1],A]$. 选择 $n\in Z$, 使 $[B,A;n]=1$, 且 n 极小, 则 $n\geq 3$. 今令 $x\in[B,A,n-3]$ 且 $[x,A,A]\neq 1$. 则 $[x,A]\nleq A$. 令 $M=[x,A]$, 则 $M\leq B$, 故 $M'\leq Z(J(P))$ 且 $[M',A]=1$, 又 $[M,A,A]=[x,A,A,A]=1$. 由引理 4.11, M 交换.

由定理 4.9, $A^*=MC_A(M)\in\mathcal{A}(P)$. 因 $[x,A,A,A]=1$, 则 $[A^*,A,A]=1$, 从而 A^* 正规化 A.

进而 $[A\cap B,A,B]=1=[B,A\cap B,A]$. 由三子群引理 $[A,B,A\cap B]=1$ 故 $A\cap B\leq C_A([A,B])\leq C_A(M)$. 但 $M\nleq A\cap B$, 从而 $A\cap B\lneqq A^*\cap B$. 证完. □

推论 4.13 *在 4.12 假定之下. 有 $A\in\mathcal{A}(P)$ 能使 B 正规化 A.*

证 由定理 4.12, 仅需选择 $A\in\mathcal{A}(P)$, 使 $A\cap B$ 极大即可. □

定理 4.14 (Glauberman) *令 B 为 p-稳定群 G 的非平凡正规 p-子群, p 为奇素数. 若 $P\in\mathrm{Syl}_p(G)$, 则 $B\cap Z(J(P))\trianglelefteq G$.*

证 假定对于 G 定理不成立, 且 B 为使定理不真的具有极小阶的 G 的正规子群.

令 $Z = Z(J(P))$, B_1 为 $Z \cap B$ 在 G 中的正规闭包. 因 $B \trianglelefteq G$, 则有 $B_1 \leq B$, 故 $Z \cap B_1 = Z \cap B$. 由 B 的极小选择, 必有 $B = B_1$.

因 $B' \lneqq B$, 故 $Z \cap B' \trianglelefteq G$, 又 $[Z \cap B, B] \leq Z \cap B'$. 故 $\forall x \in G$, 有 $[(Z \cap B)^x, B] = [Z \cap B, B]^x \leq (Z \cap B')^x \leq Z \cap B'$. 由于 B 由所有的 $(Z \cap B)^x$ 生成, 故 $B' \leq Z \cap B'$, 即 $B' \leq Z$. 特别地, $B \cap Z$ 中心化 B', 这表明, B 本身中心化 B', 即 $B' \leq Z(B)$ 故 $cl(B) \leq 2$, 且 $B' \leq Z(J(P))$. 故对 B 可用 4.12 和 4.13.

令 L 为 G 的能正规化 $Z \cap B$ 的极大正规子群, 则 $P \cap L \in \mathrm{Syl}_p(L)$. 因 $J(P \cap L)$ char $P \cap L$, 故 $G = LN$, 其中 $N = N_G(J(P \cap L))$. 若 $J(P) \leq P \cap L$, 则 $J(P) = J(P \cap L)$, 故 N 正规化 Z, 从而也正规化 $Z \cap B$. 这就得 $Z \cap B \trianglelefteq LN = G$ 矛盾. 故假定 $J(P) \nleq L \cap P$.

由 4.13 及 4.8(2), 有 $A \in A(P)$, 能使 $[B, A, A] = 1$. 因 $B \trianglelefteq G$, 且 G 为 p-稳定, 则有 $AC/C \leq O_p(G/C)$, 其中 $C = C_G(B)$. 因 C 也中心化 $Z \cap B$, 故 $LC \trianglelefteq G$ 且 LC 正规化 $Z \cap B$. 由 L 的极大选择, 必有 $C \leq L$, 故 $AL/L \leq O_p(G/L)$. 实际上, $O_p(G/L) = 1$. 因若令 K 为 $O_p(G/L)$ 在 G 中的原像, 则 $P \cap K \in \mathrm{Syl}_p(K)$, 从而 $P \cap K$ 映到 $O_p(G/L)$ 上, 故 $K = L(P \cap K)$, 但 $P \cap K$ 正规化 $Z \cap B$, 从而就有 $P \cap K \leq L$, 故得 $K = L$, 即 $O_p(G/L) = 1$, 由此得 $A \leq L$, 而这表示 $J(P \cap L) \leq J(P)$. 由 $Z \leq A \leq J(P \cap L)$ 便得 $Z \cap B \leq Z(J(P \cap L))$. 令 $X = Z(J(P \cap L))$, 则有 $G = LN_G(X)$. 由于 L 正规化 $Z \cap B$, 故 $Z \cap B$ 在 G 中的正规闭包包含在 X 之中, 特别地, B 交换.

由于 $J(P) \nleq L \cap P$, 则有 $A_1 \in A(P)$, 且 $A_1 \nleq L$. 我们断言 $[B, A_1, A_1] \neq 1$, 否则对 A_1 重复上述讨论便得 $A_1 \leq L$, 与 A_1 之选择相矛盾.

最后, 在所有的这样的 A_1 中选择一个, 使得 $|A_1 \cap B|$ 最大. 由 4.8(2), B 不正规化 A_1, 从而由 4.10, 存在 $A^* \in A(P)$, 能使 $A_1 \cap B \lneqq A^* \cap B$ 且 A^* 正规化 A_1. 由 A_1 的极大选择, 必有 $A^* \leq P \cap L$. 从而有 $X = Z(J(P \cap L)) \leq A^*$. 但 $B \leq X$, 故有

$[B, A_1, A_1] \le [X, A_1, A_1] \le [A^*, A_1, A_1] = 1$, 矛盾. □

现在可以很容易地证明 ZJ-定理.

定理 4.15 (Glauberman ZJ-定理). 令 G 是有限群, 其中 $O_p(G) \neq 1$. 设 G 为 p-约束并且是 p-稳定的, p-为奇素数. 若 $P \in \mathrm{Syl}_p(G)$, 则 $G = O_{p'}(G)N_G(Z(J(P)))$. 特别地, 若 $O_{p'}(G) = 1$, 则 $Z(J(P)) \trianglelefteq G$.

证 我们仅须对 $G/O_{p'}(G)$ 证明相应的结论. (这时需验证 $G/O_{p'}(G)$ 仍为 p-约束和 p-稳定的, 见本章末习题 11.) 因此, 不失一般性, 可假定 $O_{p'}(G) = 1$. 由定理 4.4, $Z(J(P)) \le O_p(G)$. 于定理 4.14 中令 $O_p(G)$ 为 B, 则 $Z(J(P)) = Z(J(P)) \cap B \trianglelefteq G$. □

我们利用 ZJ-定理证明如下定理, 这一定理在奇数阶定理的证明中有着直接应用.

定理 4.16 令 G 为有限群. 对于任意奇素数 p, G 的任意 p-子群的正规化子 L 既是 p-稳定又是 p-约束的, 并且 $O_{p'}(L) = 1$. 若 $P \in \mathrm{Syl}_p(G)$, 则对于 $1 \neq Q \le P$, 必有 $N_G(Q) \le N_G(Z(J(P)))$.

证 我们证明如下稍强的结论. 即若 $T \neq 1$ 为 G 的 p-子群, 则 $N_G(T) \le N_G(Z(J(P)))$ 或 $N_G(T) \cap P = 1$. 假定结论不真. 令 $M = N_G(Z(J(P)))$, $H = N_G(T)$. 并假定 $H \not\le M$ 且 $Q = P \cap H \neq 1$, 我们可选择 H 使 Q 具有极大的阶.

我们先证, 这时 $Q \in \mathrm{Syl}_p(H)$. 若 $Q = P$, 则显然成立. 故假定 $Q < P$, 则 $Q < N_P(Q)$. 由 H 的选择, 可知 $N_G(Q) \le M$. 特别地, 若 $Q \le R \in \mathrm{Syl}_p(H)$, 则 $N_R(Q) \le M \cap H$. 由于 $P \in \mathrm{Syl}_p(M)$, 则有 $x \in M$ 能使 $(N_R(Q))^x \le P$. 若 $N_R(Q) > Q = P \cap H$, 则由 H 的选择必然有 $H^x \le M$ 即 $H \le M$, 矛盾. 故 $N_R(Q) = Q$, 这表明 $Q = R \in \mathrm{Syl}_p(H)$.

由定理之条件, 可对 H 用 ZJ-定理, 即有 $Z(J(Q)) \trianglelefteq H$. 令 $N = N_G(Z(J(Q)))$, 则 $H \le N$. 若 $Q = P$, 便有 $N = M$, 这是不可能的. 故 $Q \lneq P$, 从而 $N_P(Q) > Q$. 但显然 $Z(J(Q)) \trianglelefteq N_p(Q)$. 从

而 $N_p(Q) \leq N$. 则 $P \cap N > Q$, 故 $N \leq M$, 由此又得 $H \leq M$, 矛盾. □

§5. Glauberman-Thompson p-幂零准则

本章中我们证明著名的 Glauberman-Thompson 正规 p-补定理. 这一定理在有限群理论中有着广泛的应用.

定理 5.1 (Glauberman-Thompson) *设 G 为有限群, p 为奇素数, $P \in \mathrm{Syl}_p(G)$. 若 $N_G(Z(J(P)))$ 有正规 p-补, 则 G 也有正规 p-补.*

证 对 $|G|$ 施行归纳. 可设 G 的任意包含 P 的真子群都有正规 p-补. 假定定理不真, 则由 Frobenius 定理, 必有 G 的非平凡 p-子群 H 能使 $N_G(H)$ 没有正规 p-补. 在所有这样的子群中, 选择 H, 使 $N = N_G(H)$ 的 Sylow p-子群有最大的阶. 不失一般性可假定 $P \cap N \in \mathrm{Syl}_p(N)$.

先证明 $P \leq N$. 假定相反, 即 $P \nleq N$. 令 $R = P \cap N$, $M = N_G(Z(J(R)))$, $L = M \cap N$. 则因 $R < P$, 便有 $R < N_P(R)$. 由于 $Z(J(R))$ char R, 则 $N_P(R) \leq M$, 从而 $R < P \cap M$, 即 M 的 Sylow p-子群的阶大于 N 的 Sylow p-子群的阶, 由 H 之极大选择, M 有正规 p-补. 又因 $L \leq M$, L 也有正规 p-补. 另一方面, 因 $P \nleq N$, 故 $N < G$, 则由归纳假定, N 有正规 p-补, 与 H 的选择相矛盾. 这就证明了 $P \leq N$. 这表明 $N = G$, 否则, 由归纳假定, N 有正规 p-补.

由于我们的假设条件也适用于 $G/O_{p'}(G)$, 故若 $O_{p'}(G) \neq 1$, 则由归纳假定, $G/O_{p'}(G)$ 有正规 p-补, 从而 G 也有正规 p-补. 故 $O_{p'}(G) = 1$. 因 $G = N_G(O_p(G))$, 故不失一般性可假定 $H = O_p(G)$. 若 $H = P$, 则 $Z(J(P))$ char $P \trianglelefteq G$, 从而 $G = N_G(Z(J(P)))$ 有正规 p-补, 故 $H < P$.

令 $\overline{G} = G/H$, $\overline{P}$ 表示 P 在 $\overline{G}$ 中的像, 显然 $\overline{P} \neq 1$. 令 $\overline{N}_1 = N_{\overline{G}}(Z(J(\overline{P})))$, 并令 N_1, H_1 为 $\overline{N}_1$ 及 $Z(J(\overline{P}))$ 在 G 中的原像. 则

$N_1 = N_G(H_1)$，且 $H < H_1$，从而有 $P < N_1 < G$，由归纳假定，N_1 从而 $\overline{N}_1$ 有正规 p-补．又由归纳假定，可知 $\overline{G}$ 有正规 p-补．

以上讨论表明，$G = O_{p,p',p}(G)$，特别地，G 为 p-可解群．

由 VII,3.1 可知，若 q 为 $|\overline{G}|$ 的任意素因子，则 $\overline{P}$ 正规化某个 $\overline{Q} \in \mathrm{Syl}_q(O_{p'}(\overline{G}))$．显然 $\overline{P}$ 也正规化 $Z(\overline{Q})$．令 G_1 为 $\overline{P}Z(\overline{Q})$ 在 G 中的原像，则 $G_1 = PQ_1$，此处 $Q_1 \cong Z(\overline{Q})$．若 $G_1 < G$，则由归纳假定，G_1 有正规 p-补，即为 Q_1．特别地，$Q_1 \trianglelefteq G_1$．这样就有 $[H, Q_1] \leq H \cap Q_1 = 1$．又由 G 的 p-可解性知，$Q_1 \leq C_G(H) \leq H$，这意味着 $Q_1 = Q_1 \cap H = 1$．由以上讨论，便得 $G = G_1 = PQ_1$．

若 $p \geq 5$，则显然 G 的任何子群的商群都不同构于 $SL_2(p)$．若 $p = 3$，则 $2 \in p'$，且由上可知，G 的 p'-Hall 子群 Q_1 为可换群，故 G 中任何子群的商群不同构于 $SL_2(3)$．则由推论 4.3，可知 G 为 p-稳定的，又显然 G 是 p-约束的．于是由 $O_{p'}(G) \neq 1$，根据 ZJ-定理，便得 $Z(J(P)) \trianglelefteq G$，而由假定 $G = N_G(Z(J(P)))$ 有正规 p-补，矛盾．这就证明了定理．□

§6.　Burnside $p^a q^b$-定理

作为 ZJ-定理和前一章所讲述的结果的应用，我们将在本节中给出 Burnside $p^a q^b$-定理的一个群论证明．首先讲述一些预备性的结果．

定理 6.1　(Baer) *设 x 是有限群 G 的一个 p-元素，则 $x \in O_p(G)$ 当且仅当对任意的 $g \in G$，有 $\langle x, x^g \rangle$ 是 G 的 p-子群．*

证　$\Longrightarrow$: 设 $x \in O_p(G)$．因 $O_p(G) \lhd G$，故对任一 $g \in G$，有 $x^g \in O_p(G)$．于是 $\langle x, x^g \rangle \leq O_p(G)$，当然是 G 的 p-子群．

$\Longleftarrow$: 设 K 是 G 中包含 x 的共轭类．则对 K 中任二元素 x^a，x^b，$a, b \in G$，有 $\langle x^a, x^b \rangle = \langle x, x^{ba^{-1}} \rangle^a$ 也是 G 的 p-子群．

现在假定 G 是使结论不真的最小阶反例，$P \in \mathrm{Syl}_p(G)$．首先我们看到 $\langle K \rangle$ 不是 p-群．若否，则因 $\langle K \rangle \trianglelefteq G$，必有 $\langle K \rangle \trianglelefteq O_p(G)$，与 G 是反例矛盾．因此我们有 $K \not\subseteq P$．取 $y \in K \backslash P$，并设 $Q \in \mathrm{Syl}_p(G)$，且 $y \in Q$．则自然有 $K \cap P \neq K \cap Q$．

在 G 的所有 Sylow p-子群中选出 P, Q 使得 $K \cap P \neq K \cap Q$, 且 $|K \cap P \cap Q|$ 最大. 由 Sylow 定理, 有 $g \in G$ 使 $P^g = Q$. 于是 $(K \cap P)^g = K^g \cap P^g = K \cap Q$. 特别地, $|K \cap P| = |K \cap Q|$. 这推出 $K \cap P \not\subseteq Q$, $K \cap Q \not\subseteq P$. (因若不然, 譬如有 $K \cap P \subseteq Q$, 则 $K \cap P \subseteq K \cap Q$. 比较阶即得 $K \cap P = K \cap Q$, 矛盾.)

令 $D = \langle K \cap P \cap Q \rangle$, 自然 $D \leq P \cap Q$ 是 p-群. 取群列

$$D = P_0 < P_1 < \cdots < P_n = P,$$

使得 $|P_{i+1} : P_i| = p, i = 0, 1, \cdots, n-1$. 因为 $K \cap P \not\subseteq Q$, 但 $D \leq Q$, 故 $K \cap P \not\subseteq D$. 于是 $K \cap P \supsetneqq K \cap D$. 我们选 i 为满足 $K \cap P_i \supsetneqq K \cap D$ 的最小正整数. 取 $u \in K \cap P_i$, 但 $u \notin K \cap D$. 因为 $P_{i-1} \lhd P_i$, 有 u 正规化 P_{i-1}, 因而也正规化 $\langle K \cap P_{i-1} \rangle = \langle K \cap D \rangle = D$. 这样, 我们选出的元素 $u \in (K \cap P) \setminus Q$, 又正规化 D. 由对称性, 也可选到元素 $v \in (K \cap Q) \setminus Q$, 亦正规化 D.

现在令 $H = \langle u, v \rangle$. 由定理假设, H 是 p-群. 又由 u, v 的选择, $H \leq N_G(D)$, 于是 $HD = \langle u, v, D \rangle$ 也是 p-群. 设 $R \in \mathrm{Syl}_p(G)$, 且 $R \geq HD$. 则由 $\langle u, D \rangle \leq R \cap P$ 及 $|K \cap P \cap Q|$ 的极大性有 $K \cap R = K \cap P$. 同理, 由 $\langle v, D \rangle \leq R \cap Q$ 又得到 $K \cap R = K \cap Q$, 于是 $K \cap P = K \cap Q$, 矛盾. □

定理 6.2 *设群 G 的对合 $x \notin O_2(G)$. 则存在 G 的奇数阶元素 $a \neq 1$ 使得 $a^x = a^{-1}$. 特别地, 若 G 是非交换单群, 对 G 的任意对合都有上述性质.*

证 因 $x \notin O_2(G)$, 由定理 6.1, 存在 $g \in G$ 使得 $H = \langle x, x^g \rangle$ 不是 2-群. 但因 H 由二对合生成, 故为二面体群. 于是若令 $d = x \cdot x^g$, 则 $d^x = d^{-1}$ 且 $o(d)$ 不是 2 的方幂. 取 d 的适当方幂 $a = d^i$, 可使 $o(a)$ 为大于 1 的奇数. 于是有

$$a^x = (d^i)^x = (d^x)^i = d^{-i} = (d^i)^{-1} = a^{-1}. \qquad \square$$

在 I, 例 7.3 中证明了若有限群 G 的所有极大子群皆共轭, 则 G 必为循环 p-群. 下面的定理讨论了具有两个极大子群共轭类的有限群.

定理 6.3 设有限群 G 的极大子群恰有两个共轭类，则 G 可解.

证 设 L 和 K 是这两个极大子群共轭类的代表. 若 L 和 K 皆正规，则由 IV, 定理 2.7, G 是幂零群，当然可解. 设 L 和 K 中有一个正规，譬如 $L \trianglelefteq G$, 另一个 K 不正规. 取素数 $p \mid |G:K|$, $P \in \mathrm{Syl}_p(G)$. 则必有 $P \trianglelefteq G$. (若否，则 $N = N_G(P)$ 是 G 的真子群，于是 $N \le L$. 由 II, 命题 2.5 有 $N_G(L) = L$, 与 $L \trianglelefteq G$ 矛盾.) 令 $\overline{G} = G/P$. 则易见 $\overline{G}$ 只有一个极大子群的共轭类. 由，例 7.3 有 $\overline{G}$ 可解，从而 G 可解. 故下面我们可设 L 和 K 均非 G 的正规子群.

令 $|G:L| = r$, $|G:K| = s$. 首先我们有 $(r,s) = 1$. (若否，取素数 $p \mid (r,s)$, $P \in \mathrm{Syl}_p(G)$. 则 P 不含于 L, 也不含于 K, 于是 G 必有第三个极大子群的共轭类，矛盾.) 于是我们有对任意的 $x, y \in G$,

$$|G : L^x \cap K^y| = |G:L^x||G:K^y| = rs.$$

由此得出

$$|L^x \cap K^y| = |G|/rs = |L \cap K|, \ \forall x, y \in G. \tag{6.1}$$

不失普遍性我们可设 $r > s$. 于是有

$$|G| \ge |K^z K^w| = \frac{|K^z||K^w|}{|K^z \cap K^w|} = \frac{|G|^2}{s^2|K^z \cap K^w|}, \ \forall z, w \in G.$$

这又推出

$$|K^z \cap K^w| \ge |G|/s^2 > |G|/rs = |L \cap K|, \ \forall z, w \in G. \tag{6.2}$$

如果我们能证明对任意的素数 p, 都有

$$|K^z \cap K^w|_p \le |L \cap K|_p, \ \forall z, w \in G, \tag{6.3}$$

这将推出 $|K^z \cap K^w| \le |L \cap K|$, 矛盾于 (6.2) 式. 于是便完成了定理的证明. 下面我们来证明 (6.3) 式.

取 K 的两个共轭子群 $K^{z_0} \neq K^{w_0}$ 使 $|K^{z_0} \cap K^{w_0}|_p$ 达到最大. 不失普遍性可设 $z_0 = 1$ 且 $|K \cap K^{w_0}|_p > 1$. 取 $P \in \mathrm{Syl}_p(K \cap K^{w_0})$, $P_1 \in \mathrm{Syl}_p(K)$ 使 $P_1 \geq P$. 令 $N = N_G(P)$. 则有 $N \neq G$. (若否, 有 $P \trianglelefteq G$. 作商群 $\overline{G} = G/P$. 用对 $|G|$ 的归纳法可完成定理的证明.) 设 M 是 G 的一个包含 N 的极大子群. 我们讨论下述三种情形:

(1) $P_1 > P$: 此时有 $M \cap K \geq N \cap K = N_K(P)$. 因 $P_1 > P$ 有 $|M \cap K|_p > |P|$. 同理有 $|M \cap K^{w_0}|_p > |P|$. 由 K^{w_0} 的选择, 知 M 不与 K 共轭. 这样 $M = L^x$ 对某个 $x \in G$ 成立. 由 (6.1) 式,

$$|L \cap K|_p = |M \cap K|_p > |P| = |K \cap K^{w_0}|_p,$$

(6.3) 式成立.

(2) $P_1 = P \notin \mathrm{Syl}_p(G)$: 此时有 $p \mid |G:K|$, 因此 $p \nmid |G:L|$. 这推出 $|L|_p = |G|_p > |P|$. 由 (6.1) 式有 $|L \cap K|_p = |P| = |M \cap K^{w_0}|_p$, (6.3) 式成立.

(3) $P_1 = P \in \mathrm{Syl}_p(G)$: 设 M 与 K 共轭. 不失普遍性可设 $M = K^{w_0}$. 因 $P \leq K^{w_0}$ 和 $P^{w_0} \leq K^{w_0}$, 有 $k \in K^{w_0}$ 使 $P = P^{w_0 k}$. 于是 $w_0 k \in N_G(P) \leq K^{w_0}$. 这推出 $w_0 \in K^{w_0}$, $K = K^{w_0}$, 矛盾. 于是有 $M = L^x$ 对某个 $x \in G$ 成立. 这样 $|L|_p = |K|_p = |G|_p$, 由 (6.1) 式, 我们有 $|L \cap K|_p = |P| = |K \cap K^{w_0}|_p$, (6.3) 式成立. □

定理 6.4 (Burnside) 设 p, q 是二互异素数, a, b 是正整数. 则 p^aq^b 阶群可解.

证 设 G 是使定理不真的最小阶群. 则显然 G 是非交换单群, 并且 G 的每个真子群都是可解的. 我们将分析 G 的结构, 最终得出一个矛盾, 从而证明了定理.

用 $\mathcal{M}$ 表 G 的所有极大子群的集合, 则 $\mathcal{M}$ 的每个元素都是可解的. 为方便起见, 我们用 r 表示 p 或 q, 并对 G 的子群 H, 用 H_r 表 H 的 Sylow r-子群. 则有 $H = H_r H_{r'}$.

设 $M \in \mathcal{M}$. 则因 M 可解, 有 $F(M) \neq 1$. 若 M 有非平凡正规子群 N, 则因 M 是单群的极大子群, 有 $N_G(N) = M$ 且 $C_G(N) = C_M(N)$. 下面分步来证明定理.

(1) 设 $U \le G_r$ 且 U 被 $G_{r'}$ 正规化, 即 $U^{G_{r'}} = U$, 则 $U = 1$: 因为 $G = G_{r'}G_r$, 我们有

$$U^G = U^{G_{r'}G_r} = U^{G_r} \le G_r < G.$$

又因 G 是单群, $U^G \lhd G$, 有 $U^G = 1$. 于是 $U = 1$.

(2) 设 $M \in \mathcal{M}$. 如果 $F(M)_p \ne 1 \ne F(M)_q$, 并令 $Z = Z(F(M))$, 则 M 是 G 的包含 Z 的唯一的极大子群: 假定 $Z \le L \in \mathcal{M}$. 因为 $Z \lhd M$, $Z = Z_r \times Z_{r'}$, 我们有 $1 \ne Z_r \lhd M$. 又因 $Z \le L$, 我们有

$$Z_r \lhd M \cap L = N_G(Z_{r'}) \cap L = N_L(Z_{r'}), \tag{6.4}$$

即 $Z_r \le O_r(N_L(Z_{r'}))$. 于是由 VII,3.13 有 $Z_r \le O_r(L)$. 同理有 $Z_{r'} \le O_{r'}(L)$, 于是 $Z \le F(L) = O_r(L) \times O_{r'}(L)$. 由此推出

$$O_r(L) \le C_G(Z_{r'}) = C_M(Z_{r'}) \le M.$$

同理 $O_{r'}(L) \le M$. 这推出 $F(L) \le M$. 因为 $Z \le F(L)$, 有 $F(L)_p \ne 1 \ne F(L)_q$. 应用同样的推理于 L, 又得到 $F(M) \le L$. 现在在 (6.4) 式中用 $F(M)_r$ 和 $F(M)_{r'}$ 代替 Z_r 和 $Z_{r'}$, 就得到 $F(M) \le F(L)$. 由对称性又有 $F(L) \le F(M)$, 于是 $F(M) = F(L)$. 因此有

$$M = N_G(F(M)) = N_G(F(L)) = L.$$

(3) 设 $M \in \mathcal{M}$. 则 $F(M)$ 是 p-群或 q-群: 用反证法. 假定 $F(M)$ 既不是 p-群也不是 q-群. 则前面已证 M 是 G 的包含 $Z = Z(F(M))$ 的唯一的极大子群. 设 $1 \ne z \in Z$, 我们有 $C_G(z) \ge Z$, 于是

$$C_G(z) \le M, \quad \forall z \in Z \setminus \{1\}. \tag{6.5}$$

取 M_r 和 G_r 使得 $M_r \le G_r$. 因 M_r 正规化 $F(M)_{r'} \ne 1$, 但由 (1) G_r 不正规化 $F(M)_{r'}$, 有 $M_r < G_r$. 于是存在 r-元素 $g \in N_G(M_r) \setminus M$ 使得

$$M_r^g = M_r, \quad M^{g^{-1}} \ne M. \tag{6.6}$$

现在我们断言 Z 必为循环群，这只须证 Z_r 是循环群. 假定 Z_r 不循环，因 $Z_r \leq M_r = M_r^g \leq M^g$, 考虑 Z_r 共轭作用在 $S = O_{r'}(M^g)$ 上，由 VII,3.15 有

$$S = \langle C_S(z) \mid z \in Z_r \setminus \{1\} \rangle.$$

于是由 (2) 有 $S \leq M$. 另一方面，有

$$O_r(M^g) \leq M_r^g = M_r \leq M,$$

于是 $F(M^g) = O_r(M^g) \times S \leq M$. 用 g^{-1} 共轭作用又得 $F(M) \leq M^{g^{-1}}$. 但因 $F(M) \geq Z$, 由 (2) 有 $M^{g^{-1}} = M$, 与 (3) 矛盾，于是 Z 是循环的.

现在我们设 $p < q$, 且 $g \in G$ 满足

$$M_q^g = M_q, \quad M^{g^{-1}} \neq M. \tag{6.6'}$$

因为循环群 $Z_p^g = Z(F(M^g)_p)$ 被 $Z_q \leq M_q \leq M^g$ 正规化，我们得到 $Z_q/(C_G(Z_p^g) \cap Z_q)$ 同构于 $\mathrm{Aut}(Z_p^g)$ 的子群. 但因 $q \nmid |\mathrm{Aut}(Z_p^g)| = p^i(p-1)$, 有 $Z_q = C_G(Z_p^g) \cap Z_q$. 于是有 $Z_q \leq C_G(Z_p^g)$, 又有 $Z_p^g \leq C_G(Z_q) \leq M$. 另一方面，由 $Z_q^g \leq M_q^g = M_q \leq M$ 有 $Z^g = Z_p^g \times Z_q^g \leq M$, 因此 $Z \leq M^{g^{-1}}$. 由 (2) 我们即可得到 $M^{g^{-1}} = M$, 矛盾于 (6.6′) 式.

(4) 设 $M \in \mathcal{M}$. 如果存在 G 的 Sylow r-子群 G_r 使得 $Z(G_r) \cap M \neq 1$, 则 $F(M)$ 是 r-群：假定 $F(M)$ 不是 r-群，则由 (3) 必为 r'-群. 取 $G_{r'} \geq F(M)$. 由 V,4.3(3), 有

$$Z = Z(G_{r'}) \leq C_G(F(M)) \leq C_M(F(M)) \leq F(M).$$

令 $Y = Z(G_{r'}) \cap M$. 我们有

$$Z^Y = \langle Z^y \mid y \in Y \rangle \leq F(M)^M = F(M).$$

用 $\mathcal{X}$ 表 G 的所有满足下列条件的子群 X 的集合：

$$X = X_{r'} = X^Y = \langle Z^g \mid g \in G, Z^g \leq X \rangle.$$

则 $Z^Y \in \mathcal{X}$. 取 $\mathcal{X}$ 的一个极大元 X_0 和 G 的一个 Sylow r'-子群 $\overline{G}_{r'} \geq X_0$. 因为 $Y \lhd G_r$ 和 $G = G_r\overline{G}_{r'}$, 我们有

$$1 \neq Y^G = Y^{G_r\overline{G}_{r'}} = Y^{\overline{G}_{r'}} \leq \langle Y, \overline{G}_{r'} \rangle.$$

由 G 的单性这推出 $\langle Y, \overline{G}_{r'} \rangle = g$. 我们断言 $X_0^{\overline{G}_{r'}} \neq X_0$. (若否, 因 $X_0^Y = X_0 X_0^{\langle Y, \overline{G}_{r'} \rangle} = X_0^G = X_0$, 我们将有 $X_0^{\langle Y, \overline{G}_{r'} \rangle} = X_0^G = X_0$, 于是 $X_) \lhd G$, 矛盾于 G 的单性.) 于是 $N_{\overline{G}_{r'}}(X_0) < \overline{G}_{r'}$, 并且存在元素 $u \in N_{\overline{G}_{r'}}(N_{\overline{G}_{r'}}(X_0)) \setminus N_{\overline{G}_{r'}}(X_0)$ 使得

$$X_0 \neq X_0^u \leq N_{\overline{G}_{r'}}(X_0) \leq N_G(X_0).$$

因 $X_0 \leq N_G(X_0)$ 且 $X_0 = \langle Z^g \mid Z^g \leq X_0 \rangle$, 存在 $a \in G$ 使得 $Z^a \not\leq X_0$ 和 $Z^a \leq N_G(X_0)$.

令 $A = (Z^a)^Y$, 我们将证 $AX_0 \in \mathcal{X}$. 因为

$$\begin{aligned}(AX_0)^Y = A^Y X_0^Y = AX_0 &= (Z^a)^Y \langle Z^g \mid Z^g \leq X_0 \rangle \\ &= \langle Z^g \mid Z^g \leq AX_0 \rangle,\end{aligned}$$

只须证 AX_0 是 r'-群. 又因 $A \leq \langle Z^a, Y \rangle \leq N_G(X_0)$, 又只须证 A 是 r'-群. 因为 $G = G_{r'}G_r$, 可令 $a = bc$, 其中 $b \in G_{r'}$, $c \in G_r$. 这时因 $Z = Z(G_{r'})$ 和 $Y \leq Z(G_{r'})$, 我们有

$$A = (Z^a)^Y = (Z^{bc})^Y = (Z^c)^Y = (Z^Y)^c.$$

因 Z^Y 是 r'-群得 A 是 r'-群. 这样我们有 $X_0 < AX_0 \in \mathcal{X}$, 矛盾于 X_0 的选择的极大性.

下面我们区分 $|G|$ 是偶数和奇数两种情况来找出最后的矛盾, 从而完成定理的证明. 首先设 $|G|$ 是偶数.

(5) 若 $|G|$ 是偶数, 可设 $p = 2 < q$. 设 P 是 G 的 Sylow 2-子群. 取一个对合 $t \in Z(P)$. 由定理 6.2, 存在 $1 \neq y \in G$ 使 $y^t = y^{-1}$ 且 y 的阶是 q 的方幂. 令 $Y = \langle y \rangle \leq Q \in \mathrm{Syl}_q(G)$. 取 $M \in \mathcal{M}$ 使 $M \geq N_G(Y)$. 由 $N_G(Y) \geq Z(Q)$ 我们有 $M \cap Z(Q) \neq 1$. 则由 (4) $F(M)$ 是 q-群. 但我们又有 $t \in N_G(Y) \cap Z(P) \leq M \cap Z(P) \neq 1$,

这推出 $F(M)$ 是 2-群，矛盾. 这完成了在 $|G|$ 是偶数情况下的证明.

下面我们假定 $|G|$ 是奇数. 我们分以下三步来找出一个矛盾.

(6) 设 $M \in \mathcal{M}$, 且 $F(M) = F(M)_r$. 则 $M_r \in \mathrm{Syl}_r(G)$, 并且 M 是 G 的包含 M_r 的仅有的极大子群：因为 $O_{r'}(M) = 1$, 由 ZJ-定理， $Z = Z(J(M_r)) \trianglelefteq M$, 于是又有 $M = N_G(Z)$. 假定 $M_r < G_r \in \mathrm{Syl}_r(G)$, 则 $N_{G_r}(M_r) > M_r$. 因 Z char M_r, 我们有 $N_{G_r}(Z) \geq N_{G_r}(M_r) > M_r$, 与 $M = N_G(Z)$ 相矛盾. M 的唯一性可由 $M = N_G(Z(J(M_r)))$ 得到.

(7) G 恰有两个极大子群的共轭类：我们只须证若 $F(M_1) = F(M_1)_r$ 且 $F(M_2) = F(M_2)_r$, 则 M_1 和 M_2 共轭. 设 $P_1 \in \mathrm{Syl}_r(M_1)$, $P_2 \in \mathrm{Syl}_r(M_2)$. 因 P_1 和 P_2 共轭，存在 $x \in G$ 使 $P_1^x = P_2$. 于是有

$$M_1^x = N_G(Z(J(P_1)))^x = N_G(Z(J(P_1^x))) = N_G(Z(J(P_2))) = M_2,$$

得证.

(8) 最终的矛盾：由定理 6.3 立得. □

§7. Frobenius 群

在本章的最后，我们继续研究在第 VI 章 §8 中研究过的 Frobenius 群 (以下简称 F-群). 我们曾经证明它的 Frobenius 核 (以下简称 F-核) 是一个正规子群 (见 VI, 定理 8.5). 在本节中我们将证明 F-群的 F-核是幂零群. 这曾经是一个长达半个多世纪的猜想，被著名群论学者 J.G. Thompson 在 1959 年证明. 首先我们用抽象群的办法再次给出 Frobenius 群的定义.

定义 7.1 设 G 是有限群， $1 < H < G$. 如果

$$H \cap H^g = 1, \ \forall g \in G - H, \tag{7.1}$$

(特别地，我们有 $N_G(H) = H$), 则称 G 为关于子群 H 的 F-群，并称 H 为 G 的 Frobenius 补 (以下简称 F-补). 而

$$N = G - \bigcup_{g \in H} (H^g - \{1\}) \tag{7.2}$$

叫做 G 的 F-核.

上述定义和 VI, 定义 8.4 是等价的. 因为容易验证 VI, 定义 8.4 中的置换群 G 关于稳定子群 $H=G_1$ 就满足上述定义中的条件; 并且反过来, 若有抽象群 G 和 H 满足上述定义, 则 G 在 H 的右陪集上作的传递置换表示是忠实的并满足 VI, 定义 8.4 的条件. 又, (7.2) 式中所给出的 N 恰对应于置换表示中的全体正则元素和单位元素. 因此, 由 VI, 定理 8.5, 在上述定义中的 N 也是 G 的正规子群.

下面设 G 是关于子群 H 的 F-群, $|H|=h, |G:H|=n$. 则第 VI 章 §8 告诉我们

定理 7.2 (1) $|N|=n, |G|=nh$, 且 $h \mid n-1$. 因此, H 和 N 都是 G 的 Hall 子群.

(2) 设 $G=H\cup Hg_2\cup\cdots\cup Hg_n$ 是 G 关于 H 的右陪集分解, 则

$$G=N\cup H\cup H^{g_2}\cup\cdots\cup H^{g_n}, \tag{7.3}$$

且其中任二子群的交均为 1. 我们称 (7.3) 式为 G 的 Frobenius 分解, 简称 F-分解.

为了进一步研究 F-群, 我们引进下述概念.

定义 7.3 设 G 是有限群.

(1) 称 $\alpha\in \mathrm{Aut}(G)$ 为 G 的无不动点自同构 (fixed-point-free automorphism), 简称 f.p.f. 自同构, 如果 $C_G(\alpha)=1$.

(2) 设 $A\le \mathrm{Aut}(G)$. 若 A 中每个非单位元素皆为 G 之无不动点自同构, 则称 A 为 G 的一个无不动点自同构群.

(3) 设群 H 作用在群 G 上. 若每个 $1\ne h\in H$ 都诱导出 G 的无不动点自同构, 则称 H 在 G 上的作用是无不动点的.

显然, 若 H 无不动点地作用在 G 上, 则此作用必忠实.

命题 7.4 设 G 是 F-群, H 和 N 分别是 G 的 F-补和 F-核. 则 H 依共轭变换在 N 上的作用是无不动点的. 反之, 若非平凡

群 H 无不动点地作用在非平凡群 N 上，则半直积 $S = N \rtimes H$ 是 F-群，其中 H 和 N 分别为 S 的 F-补和 F-核.

证 $\Longrightarrow$: 设 G 是 F-群. 则对任意的 $1 \neq y \in H$ 和 $1 \neq x \in N$ 有 $x \notin N_G(H)$, 于是 $H^x \cap H = 1$. 这推出 $x \notin C_N(y)$, 由 x 的任意性得 $C_N(y) = 1$, 即 y 在 N 上的作用是无不动点的.

$\Longleftarrow$: 只须对任意的 $g \in G - H$, 证明 $H \cap H^g = 1$. 设 $g = yx$, 其中 $y \in H, x \in N$. 由 $g \notin H$ 有 $x \neq 1$. 假定有 $1 \neq y_1 \in H \cap H^g = H \cap H^x$, 于是存在 $1 \neq y_2 \in H$ 使 $y_1 = y_2^x = y_2[y_2, x]$. 因 $N \lhd G$, 有 $[y_2, x] \in N$, 于是 $y_2^{-1}y_1 \in N$. 又 $y_2^{-1}y_1 \in H$, 而 $H \cap N = 1$, 故 $y_2^{-1}y_1 = 1$, 即 $y_2 = y_1$. 由此还有 $y_1 = y_1^x$, 即 $x \in C_N(y_1)$. 由 y_1 在 N 上作用无不动点以及 $x \neq 1$ 就得到 $y_1 = 1$, 矛盾. □

这个命题可以作为 F-群的又一定义.

为了进一步分析 H 和 N 的构造，我们需要无不动点自同构的下述性质.

定理 7.5 设 G 是有限群，α 是 G 的无不动点自同构，$o(\alpha) = n$. 则

(1) 若 $(m, n) = 1$, 则 α^m 也是 G 的无不动点自同构;

(2) 映射 $\mu : g \mapsto [g, \alpha] = g^{-1}g^\alpha, g \in G$ 是 G 到自身的一一映射;

(3) 若 g 和 g^α 在 G 中共轭，则 $g = 1$;

(4) $gg^\alpha \cdots g^{\alpha^{n-1}} = 1, \forall g \in G$;

(5) 若 $n = p^s$ 是素数方幂，则 G 是 p'-群.

证 (1) 由 $(m, n) = 1$, α 也是 α^m 的方幂. 故由 α 无不动点知 α^m 亦无不动点.

(2) 若 $[g, \alpha] = [g_1, \alpha]$, 即 $g^{-1}g^\alpha = g_1^{-1}g_1^\alpha$, 则 $gg_1^{-1} = (gg_1^{-1})^\alpha$. 于是 $gg_1^{-1} \in C_G(\alpha) = 1$, $g = g_1$. 这说明 μ 是单射. 而由 G 的有限性，当然 μ 也是满射.

(3) 设 $g^\alpha = g^{g_1}$, $g, g_1 \in G$. 由 (2), 存在 $x \in G$ 使 $g_1 = [x, \alpha] = x^{-1}x^\alpha$. 于是

$$g^\alpha = g^{x^{-1}x^\alpha} = x^{-\alpha}xgx^{-1}x^\alpha.$$

由此有 $(xgx^{-1})^\alpha = xgx^{-1}$. 由 $C_G(\alpha) = 1$ 得 $xgx^{-1} = 1$, 于是 $g = 1$.

(4) 令 $h = gg^\alpha \cdots g^{\alpha^{n-1}}$. 因 $\alpha^n = 1$, 有

$$h^\alpha = g^\alpha g^{\alpha^2} \cdots g^{\alpha^{n-1}} g = g^{-1}hg.$$

由 (3), 有 $h = 1$.

(5) 设 G 不是 p'-群. 则由 $\langle\alpha\rangle$ 是 p-群, 由 VII, 定理 1.9, 必存在 G 的 Sylow p-子群 P 是 α-不变的. 又由 VII, 命题 1.8, $C_P(\alpha) \neq 1$, 与 $C_G(\alpha) = 1$ 矛盾. □

定理 7.6 设 G 是有限群, α 是 G 的无不动点自同构. 如果 $N \lhd G$, $N^\alpha = N$, 则

(1) $\alpha|_N$ 是 N 的无不动点自同构;

(2) α 诱导出 $\overline{G} = G/N$ 的无不动点自同构 $\bar{\alpha}$.

证　(1) 显然.

(2) 假定 $g^\alpha N = gN$, $g \in G$. 我们要证明 $g \in N$. 由 $g^\alpha N = gN$ 有 $g^{-1}g^\alpha \in N$. 由定理 7.5(2), $g^{-1}g^\alpha = n^{-1}n^\alpha$ 对某个 $n \in N$ 成立. 由此推得 $(gn^{-1})^\alpha = gn^{-1}$, 于是 $gn^{-1} = 1$, $g = n \in N$. 这样 $\bar{\alpha}$ 是 $\overline{G}$ 的无不动点自同构. □

下面我们可以证明 Thompson 最著名的定理之一. 它解决了 Frobenius 关于 F-群的 F-核是幂零群的长达半个多世纪的著名猜想.

定理 7.7 (Thompson) 设 G 是有限群, p 是素数. 如果 G 有 p 阶无不动点自同构 α, 则 G 是幂零群.

证　设 G 是使定理不真的最小阶反例. 令 $S = G \rtimes H$, 其中 $H = \langle\alpha\rangle$ 是 p 阶循环群. 则有

(1) 若 $1 < N \lhd G$, $N < G$, 且 $N^\alpha = N$. 则 N 和 G/N 幂零: 由定理 7.6, $\alpha|_N$ 和 $\bar{\alpha}$ 分别为 N 和 G/N 的无不动点自同构. 由 $N > 1$ 和 $G/N > 1$, $\alpha|_N$ 和 $\bar{\alpha}$ 仍为 p 阶. 于是由 G 之极小性得 N 和 G/N 的幂零性.

(2) $Z(G)=1$: 若否，可设 $1<Z(G)<G$. 由 (1), $G/Z(G)$ 幂零，于是 G 亦幂零，矛盾.

(3) G 非可解，则由 (1) G 为特征单群：假定 G 可解. 在半直积 S 中取一主因子 G/Q, 则 G/Q 是初等交换 r-群. 由定理 7.5(5), G 是 p'-群. 故 $r\neq p$. 我们设 $|G/Q|=r^t$.

由 G 非幂零，有 $1<Q<G$. 又因 $Q^\alpha=Q$, 由 (1) 有 Q 幂零. 令 $Q=Q_1\times\cdots\times Q_k$, 其中 Q_i 是 Q 的 Sylow q_i-子群. 则由 Q_i char Q, 有 $1<Q_i\lhd G$ 且 $Q_i^\alpha=Q_i$. 于是由 (1) 又有 G/Q_i 幂零. 如果 $k\geq 2$, 由 G/Q_1 和 G/Q_2 幂零可得 $G/(Q_1\cap Q_2)\cong G$ 幂零，矛盾. 故必有 $k=1$, 即 Q 是 q-群，对某素数 q. 因 G 是 p'-群，有 $q\neq p$. 又因 G 非幂零，有 $q\neq r$. 再因为 $\Phi(Q)$ char Q, 如果 $\Phi(Q)\neq 1$, 则由 (1) 又有 $G/\Phi(Q)$ 幂零. 而由 IV, 推论 3.5, 因 $Q\lhd G$ 有 $\Phi(Q)\leq\Phi(G)$, 故 $G/\Phi(G)$ 幂零，从而得到 G 幂零，矛盾. 故必有 $\Phi(Q)=1$, 即 Q 是初等交换 q-群.

因为 α 是 G 的无不动点自同构，由定理 7.6(2), α 诱导出 $\overline{G}=G/Q$ 的无不动点自同构 $\bar{\alpha}$. 据命题 7.4, $\overline{S}=\overline{G}\rtimes\langle\alpha\rangle$ 为 F-群. 命 $\overline{H}=\langle\alpha\rangle$, $\overline{G}=\{\bar{1},\bar{g}_2,\cdots,\bar{g}_{r^t}\}$, 则

$$\overline{S}=\overline{G}\cup\overline{H}\cup\overline{H}^{\bar{g}_2}\cup\cdots\cup\overline{H}^{\bar{g}_{r^t}} \tag{7.4}$$

是 $\overline{S}$ 的 F-分解.

考虑 $\overline{S}$ 依共轭变换在 Q 上的作用. 对任意的 $x\in Q$, 我们用两种方法来计算 $\prod_{\bar{s}\in\overline{S}}x^{\bar{s}}$. 因为 $\overline{H}^{\bar{g}_i}=\langle\bar{g}_i^{-1}\bar{\alpha}\bar{g}_i\rangle$, 故

$$\begin{aligned}\prod_{\bar{h}\in\overline{H}^{\bar{g}_i}}x^{\bar{h}} &= \prod_{j=0}^{p-1}x^{\bar{g}_i\bar{\alpha}^j\bar{g}_i}\\ &= [(x^{g_i^{-1}})^{1+\alpha+\cdots+\alpha^{p-1}}]^{g_i}=1,\end{aligned}$$

式中 g_i 表 $\bar{g}_i$ 在 G 中的原像. 应用 (7.4) 式得到

$$\begin{aligned}\prod_{\bar{s}\in\overline{S}}x^{\bar{s}} &= \prod_{\bar{g}\in\overline{G}}x^{\bar{g}}\prod_{i=1}^{r^t}(\prod_{\bar{1}\neq\bar{h}\in\overline{H}^{\bar{g}_i}}x^{\bar{h}})\\ &= x^{-r^t}\prod_{\bar{g}\in\overline{G}}x^{\bar{g}}.\end{aligned}$$

再由 $\overline{S}$ 的右陪集分解式 $\overline{S}=\bigcup_{j=0}^{p-1}\overline{G}\bar{\alpha}^j$ 得到

$$\prod_{\bar{s}\in\overline{S}}x^{\bar{s}}=(\prod_{\bar{g}\in\overline{G}}x^{\bar{g}})^{1+\alpha+\cdots+\alpha^{p-1}}=1.$$

综合前式即得到 $x^{r^t}=\prod_{\bar{g}\in\overline{G}}x^{\bar{g}}$. 注意到 $\prod_{\bar{g}\in\overline{G}}x^{\bar{g}}\in Z(G)$, 于是 $x^{r^t}\in Z(G)$. 由 $(r^t,q)=1$, 得 $x\in Z(G)$. 而由 x 的任意性，又得 $Q\le Z(G)$, 与 (2) 矛盾. 故 G 非可解. 如果 G 有非平凡特征子群，则由 (1) 推出 G 可解，矛盾. 因此 G 是特征单群.

(4) 最终的矛盾的导出：因为 G 非幂零，故 G 不是 2-群. 取素数 $q\neq 2$, 且 $q\mid |G|$. 由 VII, 引理 3.1, 存在 G 的 α-不变的 Sylow q-子群 Q. 于是 $N_G(Z(J(Q)))$ 也是 α-不变的. 由 (3), G 是非可解特征单群，必为有限个同构的非交换单群的直积. 它没有正规 q-子群. 故 $N_G(Z(J(Q)))$ 是 G 的真子群. 于是 $N_G(Z(J(Q)))$ 幂零，当然更是 q-幂零的. 由定理 5.1, G 也是 q-幂零的，它存在正规 q-补 K. 因为 K 是 G 的非平凡特征子群，与 G 是特征单群相矛盾. □

由这个定理和命题 7.4 得

推论 7.8 *F-群 G 的 F-核是幂零群.*

关于 F-群的 F-补的构造，我们有下面的

定理 7.9 (Burnside) *设 G 是 F-群，H 是它的 F-补. 则 H 的任一 Sylow 子群或循环，或为广义四元数群.*

证 设 $p\mid |H|$, $P\in \mathrm{Syl}_p(H)$. 又设 A 是 P 的任一交换子群. 考虑 A 依共轭变换在 G 的 F-核 N 上的作用. 因为 $C_N(a)=1$, $\forall a\in A-\{1\}$, 故由 VII, 推论 3.15 推知 A 必循环. 这说明 P 中没有 (p,p) 型子群. 如果 $p\neq 2$, 由 IV,5.10(1) 即得到 P 循环. 而如果 $p=2$, 则由 IV,5.10(2) 及 IV, 定理 5.14 推知 P 或循环，或为广义四元数群. □

习　题

1. 用 Grün 第二定理和 Schur-Zassenhaus 定理证明 Burnside 定理.

2. 证明有限群 G 幂零 $\Longleftrightarrow$ 对任一素数 $p \mid |G|$, G 都是 p-幂零的.

3. 证明 Wedderburn 定理：任一有限体 K 必交换，因而是域.

4. 设 G 是有限群，p 是 $|G|$ 的最小素因子，$P \in \mathrm{Syl}_p(G)$. 假定 P 交换，且它的型不变量两两不同，则 G 是 p-幂零群.

5. 设 G 是有限群，$p > 2$. 若 G 的每个 p 阶元素皆属于中心 $Z(G)$, 则 G 是 p-幂零群. 又设 $p = 2$, 若 G 的每个 2 阶和 4 阶元素皆属于 $Z(G)$, 则 G 是 2-幂零群.

6. 举例说明只假定 G 的 2 阶元素属于 $Z(G)$ 不能推出 G 是 2-幂零的.

7. 设 G 的每个极小子群皆正规，则 G 可解，并且 G' 有正规 Sylow 2-子群 P 使得 G'/P 是幂零群.

8. 设 G 的每个 p-子群都可由 d 元生成，且 $|G|$ 和 $(p^d-1)(p^{d-1}-1)\cdots(p-1)$ 互素，则 G 是 p-幂零群.

9. 设 G 的 Sylow p-子群循环，且 $|G|$ 与 p^2-1 互素，则 G 是 p-幂零群.

10. 应用定理 3.4 证明 VII, 定理 4.3.

11. 设有限群 G 为 p-约束和 p-稳定的，$O_{p'}(G) \neq 1$. 证明 $G/O_{p'}(G)$ 也是 p-约束和 p-稳定的.

12. 设 α 是有限群 G 的无不动点自同构. 则对任意的 $p \mid |G|$, G 中存在唯一的 α-不变的 Sylow p-子群.

13. 设 H 是 F-群 G 的 F-补，且 $|H|$ 是偶数，则 $|Z(H)|$ 也是偶数.

14. 设 G 是有限群，p 是素数，$\alpha \in \mathrm{Aut}(G)$ 满足

$$gg^{\alpha}\cdots g^{\alpha^{p-1}} = 1, \quad \forall g \in G.$$

则 G 是幂零群.

第 IX 章

可解群若干专题

有限单群分类完成之后的 10 多年中，可解群的研究有了很大的发展. 群类的迅速兴起，开拓了可解群的新领域，同时也提供了新的研究方法. K. Doerk 和 T. Hawkes 的专著 "Finite Soluble Groups" 的问世，标志着这一领域的研究成果已相当丰富. 另一方面，确定一个群的可解性以及描述具有特定条件的可解群的结构仍然是群论研究的重要问题. 因此，有关这个方面的许多新的研究课题不断地被提出来，形成另一个颇具特色的研究热点. 当然，上述两个方面并不是完全独立的，而是互相渗透互相促进的.

本章前三节讲述可解群的若干经典理论，第四节到第八节介绍可解群近年来发展的几个研究专题，它们属于后一类的问题. 关于群类，由于已有前面提到的专著，而且郭文彬教授的《群类论》一书刚刚出版，因此，有关群类的成果一般地不在这里提及.

§1. 超可解群

超可解群是一类十分重要的可解群. 尽管超可解群的理论已相当成熟，但是富有创意的新成果仍在不断地被人们发现. 本节的主要任务是介绍超可解群中最为重要的那些经典结果，仅以几个较新的成果作为应用的示范.

定义 1.1 设 $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$ 是群 G 的一个主群列，G_{i+1}/G_i 为 G 的主因子. 若素数 $p \mid |G_{i+1}/G_i|$，则称 G_{i+1}/G_i

为 G 之 p-主因子.

定义 1.2 设 H 和 K 为群 G 的正规子群, $K \leq H$. 那么对每个 $x \in G$

$$f_x : hK \mapsto h^x K, h \in H$$

是 H/K 的自同构. 以 $A_G(H/K)$ 表示这些自同构的全体作成的自同构群.

命题 1.3 $A_G(H/K) \cong G/C_G(H/K)$, 其中 $C_G(H/K) = \{g \mid g \in G$ 并且 $[g,h] \in K,\ \forall h \in H\}$.

证 显然, $x \mapsto f_x$ 是 G 到 $A_G(H/K)$ 的一个群同态, 而同态核为 $C_G(H/K)$. 因此命题成立. □

定理 1.4 设 $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$ 是群 G 的主群列. 则有

(1) $F_p(G) = \bigcap\limits_{p \mid |G_{i+1}/G_i|} C_G(G_{i+1}/G_i)$ 为 p-幂零, 且为 G 的一切 p-幂零正规子群之积.

(2) G 的 Fitting 子群 $F(G) = \bigcap\limits_{i=0}^{s-1} C_G(G_{i+1}/G_i)$.

证 令

$$C = \bigcap_{p \mid |G_{i+1}/G_i|} C_G(G_{i+1}/G_i).$$

(1) 首先证明 C 包含 G 的任一正规 p-幂零子群 H, 即若 $p \mid |G_{i+1}/G_i|$, 要证 $[H, G_{i+1}] \leq G_i$. 若 $G_i > 1$, 由归纳得 $[HG_i/G_i, G_{i+1}/G_i] \leq G_i$, 从而 $[H, G_{i+1}] \leq G_i$. 因此可设 $G_i = 1$, 即 $N = G_{i+1}$ 为 G 的极小正规子群.

假设 $[H,N] \neq 1$, 则 $H \cap N \neq 1$. 于是 $N \leq H$. 因为 $N \not\subseteq O_{p'}(H)$, 又有 $N \cap O_{p'}(H) = 1$, 故知 N 为 p-群. 从而 $C_H(N) \supseteq O_{p'}(H)$ 且 $H/C_H(N)$ 为 p-群. 于是由第 VII 章命题 1.8 得 $[H,N] < N$. 因此 $[H,N] = 1$, 矛盾于假设.

现在证 C 为 p-幂零. 令 $N=G_1$ 为 G 的极小正规子群. 由归纳, $CN/N\cong C/C\cap N$ 为 p-幂零. 于是可设 $C\cap N\neq 1$. 因而 $N\le C$. 且 C/N 为 p-幂零. 若 N 为 p'-群, C 当然为 p-幂零. 设 $p\mid |N|$, 则 $[N,C]=1$, 即 $N\le Z(C)$, 故知 N 为 p-群. 令 $M/N=O_{p'}(C/N)$. 因为 C/N 为 p-幂零, 易知 C/M 是 p-群. 又因 $N\le Z(M)$ 且 N 为 M 的 Sylow p-子群, 由上册第 III 章定理 4.3 知, M 有正规 Hall p'-正规子群 L. 但是 C/L 是 p-群, 最终得 C 为 p-幂零.

(2) 显然地, $\bigcap\limits_{i=0}^{s-1} C_G(G_{i+1}/G_i)$ 是所有 $F_p(G)$ 的交, 故为正规幂零子群. 反过来要证

$$F(G)\le C_G(G_{i+1}/G_i)$$

对一切 i 成立. 因为 $F(G)G_i/G_i$ 是 G/G_i 的幂零正规子群, 当然有 $F(G)G_i/G_i\le F(G/G_i)$. 又因 G_{i+1}/G_i 是 G/G_i 的极小正规子群, 所以

$$F(G/G_i)\le C_{G/G_i}(G_{i+1}/G_i)=C_G(G_{i+1}/G_i)/G_i.$$

从而 $F(G)\le C_G(G_{i+1}/G_i)$. □

现在转入超可解群.

定义 1.5 令 p 是一个素数. 如果群 G 的主因子或为 p 阶循环群或为 p'-群, 则称 G 为 *p-超可解群*.

定义 1.6 若群 G 的主因子均为素数阶循环群, 则称 G 为 *超可解群*.

显然地, G 为超可解群当且仅当对 $|G|$ 的每个素因子 p, G 为 p-超可解群.

定理 1.7 (1) *p-超可解 (超可解) 群 G 的子群及商群也是 p-超可解 (超可解) 群.*

(2) *p-超可解 (超可解) 群的直积仍为 p-超可解 (超可解) 群.*

(3) *设 $G/N, G/K$ 均为 p-超可解 (超可解) 群, 则 $G/N\cap K$ 仍为 p-超可解 (超可解) 群.*

证 (1) 只需对 p-超可解情形证明上述结论. 令 N 为 G 的正规子群, 则 G/N 的主因子也是 G 的主因子, 因此 G/N 也是 p-超可解群.

设 $H \le G$. 令 K 为 G 的一个极小正规子群, 则 $|K|$ 或为 p 或为 p'-数. 因为 G/K 也是 p-超可解, 由归纳, HK/K 为 p-超可解. 但是 $H/H\cap K \cong HK/K$, 所以 $H/H\cap K$ p-超可解, 而 $H\cap K$ 或为 p 阶群或为 p'-群. 于是 H 的每个主因子或为 p 阶群或为 p'-群. 因此 H 为 p-超可解.

(2) 由定义推出.

(3) 不失一般性, 可设 $N\cap K = 1$. 此时 G 同构于 $G/N \times G/K$ 的一个子群, 于是结论由 (1) 与 (2) 推出. □

下述定理非常重要.

定理 1.8 (1) *G 为 p-超可解群, 则 G' 为 p-幂零群.*

(2) *G 为超可解群, 则 G' 为幂零群.*

(3) *G 为超可解群, 则 G 有 Sylow 塔性质 (见上册, 附录研究题 25). 特别地, 若 p 为 $|G|$ 的最大素因子, 则 G 有正规 Sylow p-子群.*

证 (1) 由假设, G 的 p-主因子为 p 阶循环群. 若 K/H 是这样一个主因子, 那么 $A_G(K/H)$ 作为 K/H 的自同构群的子群是循环的. 由命题 1.3, $G/C_G(K/H) \cong A_G(K/H)$ 为循环群, 于是 $G' \le C_G(K/H)$. 从而由定理 1.4 及

$$G' \le \bigcap_{p \mid |K/H|} C_G(K/H) = F_p(G)$$

得出 G' 为 p-幂零.

(2) 由 (1), 对一切 p, G' 为 p-幂零, 故 G' 幂零.

(3) 对 $|G|$ 归纳. 因为 G 为超可解, 所以 G 有素数阶正规子群 N, 记 $|N| = q$. 由定理 1.7, G/N 仍为超可解, 由归纳 G/N 有 Sylow 塔. 特别地, G/N 有正规 Sylow p-子群 PN/N. 其中 $P \in \mathrm{Syl}_p(G)$. 若 $N \le P$, 当然有 $P \lhd G$, 并且证明已完成. 设 $N \not\le P$,

则 $q < p$. 因为 p 阶群的自同构群为 $p-1$ 阶循环群, 所以 N 正规化 P, 故 $NP = N \times P$, 推出 $P \lhd G$, 结论同样成立. □

引理 1.9 令 V 为域 $GF(p)$ 上 n 维向量空间, $n \geq 1, G$ 是一个由 V 的一些线性变换作成的交换群, 方次数整除 $p-1$. 若 G 不可约地作用于 V, 那么 $n = 1$ 而 G 循环.

证　考虑 $GF(p)$ 上多项式 $f(x) = x^{p-1} - 1$ 并且令 g 是 G 的一个元素. 因 G 的方次数整除 $p-1$, 故 $f(g)$ 为零变换. 多项式 $x^{p-1} - 1$ 在域 $GF(p)$ 上可分解为线性因子之积. 因此 g 在 $GF(p)$ 上有一非零特征值 $\lambda \neq 0$, 子空间 $W = \{v \mid vg = \lambda v\} \neq 0$. 令 $x \in G, v \in W$, 则 $vxg = vgx = \lambda vgx$, 故得 $vx \in W$. 这说明 W 为 G 的非零不变子空间. 由 G 的不可约性得 $W = V$. 于是 G 的元是 V 的纯量变换. 再次应用 G 的不可约性得 $n = 1$. 又因 G 与 $GF(p)$ 的乘法群的一个子群同构, 故 G 为循环. □

定理 1.10 设 G 为 p-可解, 则 G 为 p-超可解当且仅当对 G 的每个极大子群 $M, |G:M| = p$ 或为 p'-数.

证　必要性. 对 $|G|$ 用归纳法. 因 G 为 p-超可解, 故 G 有极小正规子群 N 使得 $|N| = p$ 或为 p'-数. 令 M 是 G 的任一极大子群. 若 $N \leq M$, 则 $|G:M| = |G/N : M/N|$, 由归纳得结论成立. 设 $N \not\leq M$, 则 $G = MN, |G:M| = |N : M \cap N|$, 结论同样成立.

充分性. 假设 G 不是 p-超可解, 并且 G 是一个极小阶反例, 那么存在一 p-主因子 K 非循环. 因为 G 为 p-可解, 所以 K 为 p^n $(n > 1)$ 阶初等交换群. 由于 G 为极小阶反例, K 必定是 G 的极小正规子群, G/K 为 p-超可解.

我们断言: $F_p(G/K)$ 是一个 p-群. 由定理 1.4 知 $F_p(G/K)$ 是 G/K 的最大正规 p-幂零子群. 令 H/K 为其正规 p-补, 则 $H \lhd G$. 由上册第 III 章定理 4.3, H 有 p-补 B 使得 $H = K \rtimes B$. 由 Frattini 论断, $G = N_G(B)H = N_G(B)K$. 若 $N_G(B) < G$, 令 M 为 G 的包含 $N_G(B)$ 的一个极大子群, 则 $G = MK, M \cap K = 1$. 从而 $|G:M| = |K| = p^n, n > 1$. 矛盾于定理假设. 因此 $B \lhd G$. 若

$B > 1$, 则 G/B 为 p-超可解, 而 B 为 p'-群, 推出 G 为 p-超可解, 又一个矛盾. 于是 $B = 1$, 断言获证.

记 $P/K = (G/K)'$. 由定理 1.8(1), P/K 为正规 p-幂零群. 因 $F_p(G/K)$ 为 p-群, P/K 当然也是 p-群. 现在 G/P 为交换群, 我们知 G 有正规 Sylow p-子群. 不妨仍以 P 表示. 那么 $F_p(G/K) = P/K > 1$. 设 N/L 是 G 的 p-主因子, 使得 $K \leq L$, 则 N/L 是 p 阶群. 显然 G 中所有形如 g^{p-1} 的元中心化 N/L. 因此, 所有 $g^{p-1}K \in F_p(G/K) = P/K$, 从而 $g^{p-1}K$ 为 p-元. 于是对于 G 的任一 p'-元 g, 恒有 $g^{p-1} = 1$. 另一方面, 由上册第 III 章定理 4.3 知, G 有 p-补 U, 所以 U 的方次数整除 $p-1$. 又因 G/P 为交换, 故 U 还是交换群. 根据上册第 IV 章定理 2.9 还有 $1 < K \cap Z(P) \lhd G$. 由 K 的极小性, 得 $K \leq Z(P)$. 现在, U 不可约地作用于 K. 由引理 1.9 得出 K 为 p 阶群. 这是一个矛盾. 定理证毕. □

引理 1.11 *令 p 是群 G 的阶的最大素因子, $P \in \mathrm{Syl}_p(G)$, 那么或者 $P \lhd G$ 或者包含 $N_G(P)$ 的极大子群有合数指数.*

证 设 P 在 G 中非正规. 令 M 是 G 的任一包含 $N_G(P)$ 的极大子群. 如果 $|G:M|$ 是一个素数 r, 那么 $G/\mathrm{Core}_G(M)$ 与 S_r (r 个文字上的对称群) 的一个子群同构, 所以 r 是 $|G/\mathrm{Core}_G(M)|$ 的最大素因子. 但是 $r < p$, 我们有 $P \leq \mathrm{Core}_G(M)$. 由 Frattini 推论 $G = \mathrm{Core}_G(M)N_G(P) \leq M$. 这是一个矛盾. □

定理 1.12 (Huppert) *群 G 超可解当且仅当 G 的极大子群的指数均为素数.*

证 根据定理 1.10, 只需证充分性. 由引理 1.11, G 有正规 Sylow p-子群 P, 这里 p 为 $|G|$ 的最大素因子. 由归纳 G/P 超可解, 当然 G 为可解. 于是结论由定理 1.10 推出. □

推论 1.13 *群 G 超可解当且仅当 $G/\Phi(G)$ 超可解.*

定理 1.12 是超可解群理论中最为重要的定理, 应用很广, 现举数例如下.

令 $H \le G$, H 叫做半正规的，如果存在 $B \le G$ 使得 $G = HB$ 并且 $HX < G$ 对任意 $X < B$ 成立. 半正规是正规概念的推广.

定理 1.14 (苏向盈) *群 G 是超可解的当且仅当 G 的每个极大子群是半正规的.*

证 设 G 是超可解的，M 为 G 的极大子群，则 $|G:M| = p$, p 为某一素数. 于是 $G = M\langle x\rangle$, x 为 p-元且 $x^p \in M$. 取 $B = \langle x\rangle$, 即满足要求.

反过来，设对 G 的任一极大子群 M, 存在 $B \le G$ 使得 $G = MB$ 并且对每个 $X < B$ 恒有 $MX < G$. 由 M 的极大性，$MX = M$, 即 $X \le M \cap B$. 于是 B 有唯一极大子群而且含于 M 中. 这样的群只能是循环 p-群，并且 $|G:M| = p$. 由定理 1.12 知 G 为超可解. □

定理 1.14 虽然简单，但是它给出超可解群一个平行于幂零群的刻划. 它反映了这样一个事实：超可解群很接近幂零群.

王品超应用半正规性获得一系列关于超可解性的结果，见王品超的文章：超可解群若干充分条件，**数学学报**, **33**(1990), No. 4, 480–485.

令 $H \le G$, H 叫做 c-正规的，如果存在 $K \trianglelefteq G$ 使得 $G = HK$ 且 $H \cap K \subseteq \mathrm{Core}_G(H)$. c-正规也是正规概念的推广.

定理 1.15 (王燕鸣) *若群 G 的每个 Sylow 子群的极大子群是 c-正规的，则 G 为超可解.*

证 令 G 是一个极小阶反例.

(1) 存在素数 $p \mid |G|$ 使得 $O_p(G) \ne 1$.

假设不真. 令 p 为 $|G|$ 的最小素因子，$P \in \mathrm{Syl}_p(G)$. 设 P_1 为 P 的一个极大子群. 由假设存在 $K \trianglelefteq G$ 使得 $G = P_1K$, 且 $P_1 \cap K \le \mathrm{Core}_G(P_1) \le O_p(G) = 1$. 因此 $p^2 \nmid |K|$. 从而 K 有一个正规 p-补，当然它也是 G 的正规 p-补. 易知 K 也满足定理假设. 由归纳得出矛盾.

(2) G 有唯一的极小子群 N 使得 $G = N \rtimes M$, N 是初等交换的， M 为超可解且 $C_G(N) = N = F(G)$.

由 (1) 得 N 的存在， $N \leq O_p(G)$ 对于某个 $p \mid |G|$. 我们来证明 G/N 满足定理假设. 令 $Q \in \mathrm{Syl}_q(G)$, 则 $QN/N \in \mathrm{Syl}_q(G/N)$, q 为素数. 设 $q{\neq}p$. 对于 Q 的任一极大子群 Q_1, 存在 $K \trianglelefteq G$ 能使 $G = Q_1K, Q_1 \cap K \subseteq \mathrm{Core}_G(Q_1)$. 因为 $q{\neq}p$ 且 $K \trianglelefteq G$, 所以正规 p-子群 $N \leq K$. 于是 $Q_1N \cap KN = Q_1N \cap K = (Q_1 \cap K)N \leq \mathrm{Core}_G(Q_1)N \leq \mathrm{Core}_G(Q_1N)$. 故知 Q_1N/N 在 G/N 中 c-正规. 类似地讨论 $p = q$ 的情形. 总之 G/N 满足定理假设, 由归纳.G/N 超可解. 从而又推出 N 为唯一极小正规子群. 若 $N \leq \Phi(G)$, 由推论 1.13 知 G 为超可解. 于是可设 G 有极大子群 M 使得 $G = N \rtimes M$, M 为超可解. (2) 的余下结论显然成立.

(3) $|N| = p$, 完成证明.

令 q 为 $|G|$ 的最大素因子. 假设 $p < q$. 令 $Q \in \mathrm{Syl}_q(G)$. 因为 G/N 超可解, 所以 $QN/N \lhd G/N$ (定理 1.8), 得 $QN \trianglelefteq G$. 令 $P \in \mathrm{Syl}_p(G)$. 易知 QP 满足定理假设. 若 QP 为超可解, 由定理 1.8 得 $Q \trianglelefteq QP$. 但是 $QN = Q \times N$, 矛盾于 (2) 的结论 $C_G(N) = N$. 因此我们可设 $G = QP$. 若 $N \leq \Phi(P)$, 则由 (2), $P = P \cap (NM) = N(P \cap M) = P \cap M$. 从而 $NM = M < G$, 矛盾于 $G = NM$. 因此 $N \not\subseteq \Phi(P)$, 这意味着存在 P 的极大子群 P_1 使得 $N \not\subseteq P_1$. 由假设有 $K \trianglelefteq G$ 使 $G = P_1K, P_1 \cap K \leq \mathrm{Core}_G(P_1) \leq F(G) = N$. 由 N 的极小性得 $P_1 \cap K = 1$. 现在 $p^2 \nmid |K|$ 且 $p < q$. 因而 K 有正规 p-补 Q. 再次与 (2) 矛盾. 这样我们证明了 $p = q$.

现在 G/N 是超可解的， p 为 $|G|$ 的最大素因子, 且 $N \leq P$, 得出 $P \trianglelefteq G$. 由 (2) $N = F(G) = P$. 令 N_1 是 N 的极大子群. 由假设有 $K \trianglelefteq G$ 使 $G = N_1K$, 且 $N_1 \cap K \leq \mathrm{Core}_G(N_1)$. 由 N 的极小性得 $N_1 \leq K$, 所以 $N_1 \lhd G$. 再次由 N 的极小性得 $N_1 = 1$, 即 $|N| = p$. 完成 (3) 的证明. □

习 题

1. 设 H/K 是群 G 的主因子, $N \lhd G$ 且 $N \leq K$, 则 $A_{G/N}(H/N\big/K/N) \cong A_G(H/K)$.

2. 设 $H, K \lhd G$ 且假设 HK/K 和 $H/H\cap K$ 都是 G 的主因子, 则 $A_G(HK/K) \cong A_G(H/H\cap K)$.

3. (王品超) 若群 G 的每个 Sylow 子群半正规, 则 G 为超可解.

4. 群 G 为超可解当且仅当对于每个整除 $|G|$ 的素数 p 及每个 p-主因子 H/K, $A_G(H/K)$ 是一个循环群且方次数整除 $p-1$.

5. 设 G 为可解. 若 $F(G)/\Phi(G)$ 的每个 G-主因子为素数阶群, 则 G 为超可解群.

6. (班桂宁) 群 G 叫做严格 p-闭, 如果 G 有正规的 Sylow p-子群 P 使得 G/P 是方次数为 $p-1$ 的交换群。如果 $H \trianglelefteq G, p$ 为 $|H|$ 的最小素因子, G/H 为 p-超可解群, $p\in\pi$(素数集), H 有正规的 p-幂零 π-Hall 子群且对于 $S\in \mathrm{Syl}_p(H)$ 都有 $N_G(S)/C_G(S)$ 严格 p-闭, 则 G 为 p-超可解群.

7. (班桂宁) 令 $\pi(G)=\{p_1,p_2,\cdots,p_r\}$ 为 $|G|$ 的所有素因子的集合, $S_i\in \mathrm{Syl}_{p_i}(G)$, 如果对于每一 i 都有 $S_1\cdots S_i \trianglelefteq G$, 则 G 叫做 $(p_1\prec\cdots\prec p_r)$Sylow 塔群, 统称为 σ-Sylow 塔群。设 $H\trianglelefteq G$, G/H 超可解, H 是 σ-Sylow 塔群, 且对于 H 的每个 Sylow$p$-子群 S 都有 $N_G(S)/C_G(S)$ 严格 p-闭, 则 G 超可解.

§2. p-可解群的 p-长

定义 2.1 设 G 为 p-可解群, $1=G_0\lhd G_1\lhd\cdots\lhd G_s=G$ 是 G 的一个主群列. 若 G_{i+1}/G_i 为 p-主因子, 则令 $|G_{i+1}/G_i|=p^{n_i}$. 在所有 p-主因子中, 最大的 n_i 称为 G 的 p-秩, 记为 $r_p(G)$. $r_p(G)=0$ 等价于 G 为 p'-群; $r_p(G)=1$ 即为 p-超可解群.

由 Jordan-Hölder 定理 (上册第 III 章定理 1.5), p-秩不依赖主群列的选择.

定义 2.2 设 G 为 p-可解群. 定义 G 的上升 p-列如下:

$$1=P_0(G)\trianglelefteq M_0(G)\trianglelefteq P_1(G)\trianglelefteq M_1(G)\trianglelefteq\cdots\trianglelefteq P_l(G)\trianglelefteq M_l(G)=G$$

其中

$$M_i(G)/P_i(G)=O_{p'}(G/P_i(G)), P_i(G)/M_{i-1}(G)=O_p(G/M_{i-1}(G)).$$

我们称数 l 为 G 的 p-长度, 记为 $l_p(G)$.

由定义很容易证明 (读者自己证明)

(1) 若 $N \lhd G$, 则 $l_p(G/N) \le l_p(G)$.

(2) 若 $U \le G$, 则 $l_p(U) \le l_p(G)$.

(3) 若 $G = G_1 \times G_2$, 则 $l_p(G) = \max\{l_p(G_1), l_p(G_2)\}$.

引理 2.3 设 $N \lhd G$, $\Phi(G) \le N$ 且 $N/\Phi(G)$ 为 p-幂零, 则 N 为 p-幂零.

证 设 $K/\Phi(G)$ 为 $N/\Phi(G)$ 的正规 p-补, P 为幂零群 $\Phi(G)$ 的 Sylow p-子群. 由 Schur-Zassenhaus 定理 (上册第 III 章定理 4.3), P 在 K 中有补子群 V, 且一切补在 K 中共轭. 对于 $g \in G, V^g$ 为 P 在 K 中的补, 故 $V^g = V^h$, 而 $h \in K$. 由此得

$$G = N_G(V)K = N_G(V)VP = N_G(V)\Phi(G) = N_G(V).$$

故 V 为 N 的正规 p-补, 从而 N 为 p-幂零. □

定理 2.4 设 G 为 p-可解, 则 $l_p(G) = l_p(G/\Phi(G))$.

证 若 $l_p(G/\Phi(G)) = 0$, 则 $G/\Phi(G)$ 为 p'-群, 从而 G 为 p'-群, 于是 $l_p(G) = 0$, 结论成立.

设 $l_p(G/\Phi(G)) \ge 1$. 由引理 2.3, $F_p(G)/\Phi(G)$ 为 $G/\Phi(G)$ 的最大 p-幂零正规子群, 故 $P_1(G/\Phi(G)) = P_1(G)/\Phi(G)$. 因此对于 $i \ge 1$ 还有 $P_i(G/\Phi(G)) = P_i(G)/\Phi(G)$ 及 $M_i(G/\Phi(G)) = M_i(G)/\Phi(G)$. 由此立得 $l_p(G/\Phi(G)) = l_p(G)$. □

引理 2.5 设 G 为 p-可解, $M_0(G) = O_{p'}(G), P_1(G) = O_{p'p}(G)$. 令

$$U/M_0(G) = \Phi(P_1(G)/M_0(G)).$$

则有 $C_G(P_1(G)/U) = P_1(G)$.

证 先证 $C_G(P_1(G)/M_0(G)) \le P_1(G)$.

不妨设 $M_0(G)=1$, 即 $O_{p'}(G)=1$. 假定

$$C_G(P_1(G))P_1(G)=K>P_1(G).$$

设 $M/P_1(G) \le K/P_1(G)$ 为 $G/P_1(G)$ 的极小正规子群. 因为 $P_1(G) = O_p(G)$, 则 $M/P_1(G)$ 为 p'-群. 由 Schur-Zassenhaus 定理 (上册第 III 章定理 4.3), $P_1(G)$ 在 M 中有补 S. 故

$$M=P_1(G)\rtimes S,\ P_1(G)\cap S=1.$$

由于 $|C_G(P_1(G))P_1(G)/C_G(P_1(G))|$ 为 p 的幂, 且 $S \le C_G(P_1(G)) P_1(G)$, 故 $S \le C_G(P_1(G))$. 由此即得 $M = S\times P_1(G)$. 又因 $M \lhd G$, 得出 $S \lhd G$. 但是 S 为 p'-群, 所以 $S \le O_{p'}(G)=1$, 与 $K>P_1(G)$ 的假设矛盾.

现在来证 $C_G(P_1(G)/U)=P_1(G)$.

仍不妨设 $M_0(G)=1$, 则 $P_1(G)=O_p(G), U=\Phi(P_1(G))$, 而 $P_1(G)/U$ 为初等交换 p-群. 故 $C_G(P_1(G)/U)\ge P_1(G)$.

假定

$$C=C_G(P_1(G)/U)>P_1(G).$$

由于 $C\lhd G$, 易知 $C/P_1(G)$ 不是 p-群, 故存在 p'-元 $k\in C\backslash P_1(G)$. 由于 $k\in C_G(P_1(G)/\Phi(P_1(G)))$, 故 k 在 $P_1(G)/\Phi(P_1(G))$ 上平凡作用. 于是 k 在 $P_1(G)$ 上作用平凡. 由前一部分证明得出矛盾:

$$k\in C_G(P_1(G))\le P_1(G),$$

完成证明. □

定理 2.6 (Hall-Higman) *设 G 为 p-可解群.*

(1) *用 $c(G_p)$ 表示 Sylow p 子群 G_p 的幂零类, 则 $l_p(G)\le c(G_p)$.*

(2) *用 $d(G_p)$ 表示 G_p 的最小生成元之个数, 则 $l_p(G)\le d(G_p)$.*

(3) *用 $r_p(G)$ 表示 G 的 p-秩, 则 $l_p(G)\le r_p(G)$.*

证 (1) 对 $c(G_p)$ 用归纳法. 首先, 由于 $P_1(G)/M_0(G) = O_p(G/O_{p'}(G))$ 是一 p-群, 故 $P_1(G)/M_0(G)$ 被 $Z(G_p)$ 中心化. 由引理 2.5 得

$$Z(G_p) \le P_1(G).$$

令 $c(G_p) = 1$, 则 $G_p = Z(G_p) \le P_1(G)$, 故 $M_1(G) = G$, 从而 $l_p(G) = 1$, 结论成立.

设 $c(G_p) > 1$. 由 $Z(G_p) \le P_1(G)$ 得

$$c(G_pP_1(G)/P_1(G)) = c(G_p/G_p \cap P_1(G)) \le c(G_p) - 1.$$

由归纳得

$$l_p(G/P_1(G)) \le c(G_p) - 1.$$

从而

$$l_p(G) \le c(G_p).$$

(2) 令 P 为 $P_1(G)$ 的任一 Sylow p-子群, $P \le G_p$.

我们来证明

$$P \not\subseteq \Phi(G_p).$$

用反证法, 因为

$$\Phi(G_p)M_0(G)/M_0(G) \le \Phi(G_pM_0(G)/M_0(G)),$$

所以可以假设 $M_0(G) = 1$

现在 $P_1(G) = P \lhd G$, 且 $P_1(G) \le \Phi(G_p)$, 由上册第 IV 章定理 3.4, $P_1(G) \le \Phi(G)$. 由定理 2.4 得出矛盾:

$$l_p(G) = l_p(G/\Phi(G)) \le l_p(G/P_1(G)) = l_p(G) - 1.$$

这个矛盾证明了 $P \not\subseteq \Phi(G_p)$.

现在对 $d(G_p)$ 用归纳法. 当 $d(G_p) = 1$ 时, $c(G_p) = 1$. 由 (1) 得 $l_p(G) = 1$. 设 $d(G_p) > 1$. 由于 $P \not\subseteq \Phi(G_p)$, 故有

$$G_p \cap P_1(G) = P > \Phi(G_p) \cap P_1(G).$$

令 $d = d(G_p)$, 则

$$\begin{aligned} & |G_pP_1(G)/P_1(G) : \Phi(G_pP_1(G)/P_1(G))| \\ \leq\ & |G_pP_1(G) : \Phi(G_p)P_1(G)| \\ =\ & \frac{|G_p : \Phi(G_p)|}{|G_p \cap P_1(G) : \Phi(G_p) \cap P_1(G)|} \\ \leq\ & p^{d-1}. \end{aligned}$$

由归纳即有, $l_p(G/P_1(G)) \leq d-1$, 从而 $l_p(G) \leq d$.

(3) 令 $r_p(G) = r$. $r = 0$ 时, 结论显然成立, 故设 $r \geq 1$. 令 H/K 为 G 的一个 p-主因子, $|H/K| = p^n, n \leq r$. 由于 H/K 为 p^n 阶初等交换 p-群, 我们有 $\mathrm{Aut}(H/K) \cong GL(n,p)$(见上册第 IV 章定理 5.3 及其证明), 故 $A_G(H/K)$ 同构于 $GL(n,p)$ 的一个子群. 而 $GL(n,p)$ 的 Sylow p-子群的幂零类为 $n-1$ (作为练习, 读者自己证明), 当然 $A_G(H/K)$ 的 Sylow p-子群的幂零类不超过 $n-1$. 又因为 $A_G(H/K) \cong G/C_G(H/K)$(命题 1.3), 所以 $K_n(G_p) \leq C_G(H/K)$ ($K_n(G_p)$ 的定义见上册第 IV 章 2.1). 于是由 $n \leq r$ 知 $K_r(G_p) \leq C_G(H/K)$ 对一切 p-主因子 H/K 成立. 现在根据定理 1.4 有

$$K_r(G_p) \leq \bigcap_{p||H/K|} C_G(H/K) = F_p(G) = P_1(G).$$

从而由 (1) 得

$$l_p(G/P_1(G)) \leq c(G_pP_1(G)/P_1(G)) \leq r-1,$$

所以 $l_p(G) \leq r = r_p(G)$ 成立. □

引理 2.7 设 G 为 p-可解. 假设 G 的任一真同态像 p-长 $\leq k$, 而 $l_p(G) > k$. 则

(1) $\Phi(G) = 1$.

(2) $F_p(G) = O_{p'p}(G) = O_p(G)$ 为初等交换 p-群.

(3) $F_p(G)$ 为 G 的唯一极小正规子群且在 G 中有补.

(4) $C_G(F_p(G)) = F_p(G)$.

证 (1) 若 $\Phi(G) > 1$, 由定理 2.4 得出矛盾: $k < l_p(G) = l_p(G/\Phi(G)) \le k$, 故 $\Phi(G) = 1$.

(2) 若 $1 < K \lhd G$ 且 $p \nmid |K|$, 即得矛盾: $k < l_p(G) = l_p(G/K)$. 故 $O_{p'}(G) = 1$ 并且 $F_p(G) = O_p(G) > 1$. 由于 $\Phi(F_p(G)) \le \Phi(G) = 1$ (上册第 IV 章推论 3.5), 所以 $F_p(G)$ 为初等交换 p-群.

(3) 设 N_1, N_2 均为 G 的极小正规子群且 $N_1 \ne N_2$. 则 $l_p(G/N_1)$ 与 $l_p(G/N_2)$ 都 $\le k$, 而 G 与 $G/N_1 \times G/N_2$ 的一个子群同构, 从而推出 $l_p(G) \le k$, 矛盾于假设. 于是 G 有唯一个极小正规子群 N 且 $N \le F_p(G)$. 由于 $\Phi(G) = 1$, 有 G 的极大子群 U 能使 $G = NU$ 且 $N \cap U = 1$. 故有 $F_p(G) = N(F_p(G) \cap U)$, 且 $F_p(G) \cap U \lhd F_p(G)U = G$. 由于 N 为 G 的唯一极小正规子群, 必有 $F_p(G) \cap U = 1$. 故 $N = F_p(G)$ 且 U 为 $F_p(G)$ 的补.

(4) 若 $C_G(F_p(G)) > F_p(G)$, 则 $C_G(F_p(G)) = F_p(G) \times R$, 其中

$$1 < R = C_G(F_p(G)) \cap U.$$

由此得 $R \lhd F_p(G)U = G$, 与 N 的唯一性矛盾. □

定理 2.8 *设 G 为 p-可解群, P 为 G 的 Sylow p-子群, 而 Q 为 p-补. 若 $P'Q = QP'$, 则有 $l_p(G) \le 1$.*

证 设 G 为极小阶反例. 由于假设条件对于同态像是遗传的, 故对 $k = 1$, G 满足引理 2.7 的条件, 于是 $N = F_p(G)$ 是一个 p-群且 $N \le P$. 因此 $N \cap (P'Q) = N \cap P' \lhd P$, 且 $N \cap (P'Q) \lhd P'Q$. 由此知 $N \cap P' \lhd PQ = G$. 根据引理 2.7, N 是 G 的唯一正规子群, 所以或者 $N \cap P' = 1$ 或者 $N \le P'$.

设 $N \cap P' = 1$. 则 $[N, P'] = 1$, 从而 $P' \le C_G(N) = N$ (引理 2.7), 得出 $P' = 1$. 由定理 2.6(1) 知 $l_p(G) \le 1$ 成立.

设 $N \le P'$, 则 $N \le P' \le \Phi(P)$, 由上册第 IV 章定理 3.4 知 $N \le \Phi(G)$. 但是由引理 2.7 又有 $\Phi(G) = 1$. 这样一来, 得出 $N = F_p(G) = 1$, 这是一个矛盾. 定理证毕. □

定理 2.9 (Huppert) *设 G 为可解群, $P_1, \cdots, P_r$ 是 Sylow 系.*

(1) 若 $P_i'P_j = P_jP_i'$ 对一切 i, j 成立, 则对一切素数 p 都有 $l_p(G) \le 1$.

(2) 反过来, 若对一切素数 p 都有 $l_p(G) \le 1$, 则 P_i 的任一特征子群同 P_j 的任一特征子群可交换.

证 (1) 令 $Q_i = \prod_{j \ne i} P_j$. 则 Q_i 为 P_i 的补, 且 $P_i'Q_i = Q_iP_i'$, 于是结论由定理 2.8 得出.

(2) 设对一切素数 p 都有 $l_p(G) \le 1$. 令 $H = P_iP_j$. 易知 $l_p(H) \le l_p(G) \le 1$, 特别对 $p = p_j$ 有

$$1 \le O_{p'}(H) \le O_{p'p}(H) \le O_{p'pp'}(H) = H$$

设 U 为 P_j 的特征子群, 且令 $N = O_{p'}(H)$. 则 UN/N 为 P_jN/N 的特征子群, 从而 $NU \lhd H$. 因为 $N \le P_i$, 故知

$$P_i(NU) = P_iU$$

是 G 的子群. 因为 $l_p(P_iU) \le l_p(G) \le 1$, 同理可证对 P_i 的任一特征子群 V 有 $VU = UV$ 成立. □

习 题

1. 设 G 为 p-可解群. 证明下述诸结论:
(1) 若 $N \trianglelefteq G$, 则 $l_p(G/N) \le l_p(G)$.
(2) 若 $H \le G$, 则 $l_p(H) \le l_p(G)$.
(3) 若 $N_1, N_2 \trianglelefteq G$, 则 $l_p(N_1N_2) = \max\{l_p(N_1), l_p(N_2)\}$.

2. 设 G 为 p-可解. 若对 G 的一切 p-主因子 H/K 恒有 $|A_G(H/K)|$ 与 p 互素, 则 $l_p(G) \le 1$.

3. 设 G 为 p-可解群. 证明 G 有交换 Sylow p-子群当且仅当 $l_p(G) \le 1$ 且 $O_{p'p}(G)/O_{p'}(G)$ 为交换群.

§3. 幂零子群

在上册第 IV 章中, Schmidt 定理断言: 真子群皆为幂零的群必定可解. 本节将介绍它的一个深刻的推广, 即 Deskins-Janko-Thompson 定理.

定义 3.1 给定群 G_1,G_2 及满同态 $\mu_i: G_i \to H$. 记 Ker $\mu_i = N_i$. $G_1 \times G_2$ 的子群

$$G_1 \wedge G_2 = \{(g_1, g_2) | g_1{}^{\mu_1} = g_2{}^{\mu_2}\}$$

叫做 G_1 与 G_2 的一个次直积.

定理 3.2 在定义 3.1 的假设下, 存在同态

$$\alpha_i : G_1 \wedge G_2 \to G_i$$

满足

(1) Ker $\alpha_1 = K_1 = \{(1, n_2) \mid n_2 \in N_2\} \cong N_2$.

(2) Ker $\alpha_2 = K_2 = \{(n_1, 1) \mid n_1 \in N_1\} \cong N_1$. 还存在同态

$$\mu : G_1 \wedge G_2 \to H$$

满足

$$\text{Ker } \mu = K_1 \times K_2.$$

证 定义同态 $\pi_i : G_1 \times G_2 \to G_i$ 如下:

$$(g_1, g_2)^{\pi_i} = g_i.$$

π_i 在 $G_1 \wedge G_2$ 上的限制是 $G_1 \wedge G_2$ 到 G_i 的满同态, 记为 α_i. 显然满足

$$\text{Ker } \alpha_1 = \{(1, g_2) \mid g_2^{\mu_2} = 1\} \cong N_2.$$

$$\text{Ker } \alpha_2 = \{(g_1, 1) \mid g_1^{\mu_1} = 1\} \cong N_1.$$

同态 $\mu : G_1 \wedge G_2 \to H$ 定义为 $(g_1, g_2)^\mu = g_1^{\mu_1} = g_2^{\mu_2}$. 显然 Ker $\mu = K_1 \times K_2$. □

定理 3.3 (J.Tate) 设 P 为 G 的 Sylow p-子群, $N \lhd G$. 如果 $N \cap P \subseteq \Phi(P)$, 则 N 为 p-幂零.

证 记 $M = O^p(N) \lhd G$. 若 $M \cap P = 1$, 定理已成立, 故令 $Q = M \cap P > 1$. 由假设 $Q \subseteq \Phi(P)$.

考察

$$L = MP.$$

令 $T = \Phi(Q)$. 则由 $Q = M \cap P \lhd P$, 有 $T \lhd P$. 现在令

$$G_1 = L, N_1 = M,$$
$$G_2 = P/T, N_2 = Q/T.$$

则

$$G_1/N_1 = L/M = MP/M \cong P/M \cap P$$
$$= P/Q \cong P/T/Q/T = G_2/N_2.$$

于是有满同态 $\mu_i : G_i \to P/Q$ 能使

$$(mx)^{\mu_1} = xQ = (xT)^{\mu_2},\ \forall x \in P, m \in M.$$

作次直积

$$W = G_1 \wedge G_2 = \{(mx, xT) \mid (mx)^{\mu_1} = (xT)^{\mu_2}\}.$$

则 $\mathrm{Ker}\ \mu_1 = N_1, \mathrm{Ker}\ \mu_2 = Q/T = N_2$. 记

$$T_1 = \{(m, T) \mid m \in M = N_1\} \cong N_1,$$
$$T_2 = \{(1, qT) \mid q \in Q\} \cong N_2.$$

我们证明 W 在 T_2 上可裂. 作映射 $\varepsilon : P \to W$ 如下:

$$x^{\varepsilon} = (x, xT)\ \forall x \in P.$$

则 ε 是单同态. 设

$$(x, xT) \in P^{\varepsilon} \cap T_2.$$

立知 $(x, xT) = (1, T)$, 从而 $P^{\varepsilon} \cap T_2 = 1$. 因 $P \in \mathrm{Syl}_p(G)$, 我们有

$$|W : P^{\varepsilon}T_2| = |G_1 : P| \not\equiv 0 \pmod p.$$

故 $P^{\varepsilon}T_2$ 是 W 的一个 Sylow p 子群，而 P^{ε} 为交换正规子群 T_2 的补. 由 Gaschütz 定理 (上册第 III 章推论 4.7), W 在 T_2 上可裂.

设 R 为 T_2 在 W 中的补. 定义映射 α_1 如下:

$$r^{\alpha_1} = (g_1, g_2)^{\alpha_1} = g_1,$$

这里 $r = (g_1, g_2) \in R$. 由定理 3.2 知 $\mathrm{Ker}\ \alpha_1 \le T_2$, 故 $R \cap \mathrm{Ker}\ \alpha_1 \le R \cap T_2 = 1$. 因此 α_1 为 R 到 G_1 的同构. 设 δ 为 α_1 的逆，则 δ 为 G_1 到 W 内的同构使得

$${g_1}^{\delta} = (g_1, g_1^{\tau}),$$

其中 τ 为 G_1 到 G_2 的同态. 特别地，对于 $m \in M = N_1 \le G_1$ 成立

$$m^{\delta} = (m, m^{\tau}) \in W.$$

由 W 的定义得 $m^{\mu_1} = Q = (m^{\tau})^{\mu_2}$, 从而

$$m^{\tau} \in \mathrm{Ker}\ \mu_2 = N_2 = Q/T.$$

因此，限制 $\tau|_M$ 为 M 到 p-群 Q/T 内的同态. 因为 $M = O^p(N)$ 不具有非平凡 p-商群，故对一切 $m \in M$ 有 $m^{\tau} = T$. 从而

$$\begin{aligned} M^{\delta} &= \{(m, m^{\tau}) \mid m \in M\} \\ &= \{(m, T) \mid m \in M\} = T_1. \end{aligned}$$

由 $W = RT_2 = G_1^{\delta}T_2$ 及 $G_1^{\delta} \cap T_2 = R \cap T_2 = 1$, 及 W 到 G_2 的同态 α_2:

$$(g_1, g_2)^{\alpha_2} = g_2,\ g_i \in G_i$$

得 $G_2 = W^{\alpha_2} = (G_1^{\delta}T_2)^{\alpha_2} = G_1^{\delta\alpha_2}T_2^{\alpha_2} = G_1^{\delta\alpha_2}N_2$. 由于

$$\mathrm{Ker}\ \alpha_2 = T_1 = M^{\delta} \le {G_1}^{\delta}.$$

故由 $G_1^\delta \cap T_2 = 1$, 可得 $G_1^{\delta\alpha_2} \cap N_2 = 1$. 所以 $G_1^{\delta\alpha_2}$ 是 $N_2 = Q/T$ 在 $G_2 = P/T$ 中的补. 另一方面, 由上册第 IV 章习题第 25 题及 $Q \le \Phi(P)$ 得

$$Q/T \le \Phi(P)/T \le \Phi(P/T).$$

这与 $Q \ne T$ 矛盾, 完成证明. □

现在我们可以证明

定理 3.4 (Wielandt) *设 H 为 G 的幂零 Hall 子群但不是 Sylow 子群. 假若对于 $|H|$ 的任一素因子 p, H 的 Sylow p-子群 P 满足*

$$N_G(P) = H,$$

那么存在 $K \lhd G$ 使得 $G = KH$ 且 $K \cap H = 1$.

证 设 P 为 H 的 Sylow p-子群, p 为整除 $|H|$ 的任意固定素数. 首先证明

(1) 只要 x_1 和 $x_2 \in P$ 在 G 中共轭, 则 x_1 和 x_2 也在 P 中共轭.

事实上, 令 $x_2 = x_1^g$, 而 $g \in G$. 由于 H 不是 G 的 Sylow 子群, H 必有 Sylow q-子群 $Q > 1, q \ne p$, 能使 $x_1, x_2 \in C_G(Q)$. 又因 Q 与 Q^g 均为 $C_G(x_2)$ 的 Sylow q-子群, 故存在 $u \in C_G(x_2)$ 使得 $Q^{gu} = Q$, 从而 $gu \in N_G(Q) = H$ 且

$$x_1^{gu} = x_2^u = x_2,$$

即 x_1 与 x_2 在 H 内共轭. 再由 H 的幂零性知 x_1 与 x_2 在 P 内共轭.

(2) 对任意 $p \mid |H|$, G 为 p-幂零.

设 V 为 G 到 P/P' 内的转移. 则对于 $x \in P$

$$V(x) = \prod_j s_j x^{f_j} s_j^{-1} P',$$

其中 $s_j x^{f_j} s_j^{-1} \in P$. 由假设, 存在 $x_j \in P$ 使得

$$s_j x^{f_j} s_j^{-1} = x_j x^{f_j} x_j^{-1}.$$

故

$$V(x) = \prod_j x_j x^{f_j} x_j^{-1} P' = \prod_j x^{f_j} P' = x^{|G:P|} P'.$$

从而 $V(P) = P/P'$ 且 $\mathrm{Ker}\ V \cap P = P' \leq \Phi(P)$. 由定理 3.3, $\mathrm{Ker}\ V$ 为 p-幂零，于是 G 为 p-幂零.

(3) 导出结论.

对任意整除 $|H|$ 的素数 p, 令 $K(p)$ 为 G 的正规 p-补，再令 $K = \bigcap_p K(p)$. 则 $K \lhd G$ 且 $|G/K| = |H|$, 从而 $G = KH, K \cap H = 1$ 满足要求. □

定理 3.5 (Deskins, Janko 和 Thompson) *设 H 为 G 的极大子群. 若 H 幂零，且 H 的 Sylow 2-子群的幂零类 ≤ 2, 则 G 可解.*

证 设 G 为极小阶反例.

(1) H 为 G 的 Hall 子群并且 $\mathrm{Core}_G(H) = 1$.

假若有素数 p 能使 $1 < H_p < G_p$, 这里 H_p 与 G_p 分别为 H 和 G 的 Sylow p-子群. 由幂零群性质得

$$H < N_G(H_p) \leq G.$$

由 H 的极大性知 $H_p \lhd G$. 显然， G/H_p 与 H/H_p 一起满足定理假设，故 G/H_p 可解，从而 G 也可解，矛盾于假设. 因此 (1) 成立.

(2) H 为 G 的 Sylow 2-子群.

假设 H 不是 Sylow 子群, 则对一切素数 p 均有 $H \leq N_G(H_p) \leq G$. 因为 $\mathrm{Core}_G(H) = 1$, 则对一切 $p \mid |H|$ 总有 $N_G(H_p) = H$. 由定理 3.4 知，存在 $K \lhd G$ 使得

$$G = KH \text{ 且 } K \cap H = 1.$$

现在 π-群 H 作用在 π'-群 K 上. 由第 VII 章引理 3.1, K 有 H-不变 Sylow q-子群 $K_q > 1$. 由 H 的极大性得 $G = HK_q$, 于是从 K_q 与 G/K_q 均可解，得出 G 可解，矛盾于假设.

因此，H 是 G 的 Sylow p-子群，而 p 为某个素数. 从证明中我们还看到 G 不能是 p-幂零. 设 $U = J(H)$ (Thompson-子群)，则有 $H \leq N_G(Z(U)) < G$ (因为 $\mathrm{Core}_G(H) = 1$). 由 H 的极大性推出 $H = N_G(Z(U))$ 为 p-群. 若 $p > 2$, 由第 VIII 章定理 5.1 知 G 为 p-幂零，这是一个矛盾. 故 $p = 2$.

(3) H 的幂零类 ≥ 3.

由假设 H 的幂零类 ≤ 2. 令 $Z = Z(H)$, 则 $N_G(Z) = H$. 又因 H 的幂零类 ≤ 2, 所以 $H' \leq Z$.

我们来证明 G 是 p-正规的，这里 $p = 2$. 否则，存在 $g \in G$ 能使 $Z^g \leq H$ 但 $Z^g \neq Z$. 因 $H' \leq Z$, 故

$$H' \leq \langle Z, Z^g \rangle \leq H.$$

令 $J = \langle Z, Z^g \rangle$, 则 $J \lhd H$. 由 $Z^g \leq H$ 又得 $Z \leq N_G(Z^g) = H^g$. 因此 $J \lhd H^g$. 但是 $H \neq H^g$, 故由 H 之极大性得

$$1 < J \lhd \langle H, H^g \rangle = G,$$

与 $\mathrm{Core}_G(H) = 1$ 矛盾. 因此 G 为 p-正规.

现在应用 Grün 第二定理 (第 VIII 章定理 1.8) 即得

$$G/G'(p) \cong N_G(Z)/N_G(Z)'(p) = H/H' \neq 1.$$

因此

$$H/H' \cong G/G'(p) = G'(p)H/G'(p) \cong H/H \cap G'(p),$$

得出 $H' = H \cap G'(p)$. 若 $H' = 1$, 则 G 为 p-幂零，与 G 不是 p-幂零矛盾. 若 $H' \neq 1$, 则 $N_G(H') = H$ 且成立

$$N_{G'(p)}(H') = H \cap G'(p) = H'.$$

注意 H' 为交换群，由上册第 II 章定理 5.4 知 $G'(p)$ 为 p-幂零. 这是最后一个矛盾，定理证毕. □

注 3.6 单群 $PSL(2,17)$ 有一个 Sylow 2-子群 D 为 16 阶二面体群，幂零类为 3, 并且 D 为 $PSL(2,17)$ 的极大子群. 因此，定理 3.5 不可能再作本质上的改进.

定理 3.7 (Wielandt) 设 H 为群 G 的幂零 π-Hall 子群，则 G 的任何 π-子群 K 共轭地包含在 H 内. 特别地，G 的 π-Hall 子群彼此共轭.

证 对 K 的阶用归纳法. 令 L 是 K 的真子群，则有 $x \in G$ 使 $L^x \subseteq H$, 故 L 为幂零. 若 K 为幂零，则 K 有非平凡正规 Sylow 子群. 若 K 非幂零，则 K 为内幂零，由上册第 IV 章定理 4.2 知，K 也有非平凡正规 Sylow 子群. 因此可令 Q 为 K 的正规 Sylow q-子群，$Q > 1$. 由 Sylow 定理，Q 共轭地含于 H 的一个 Sylow q-子群中. 不失一般性，可设 $Q \le H$. 令 K_1, H_1 分别为 K 和 H 的 q-补. 则 K_1, H_1 均含于 $N_G(Q)$ 中. 由归纳，K_1 共轭地含于 H_1 中，即有 $x \in N_G(Q)$ 使得 $K_1^x \le H_1$. 因 $Q^x = Q$, 得 $K^x = (QK_1)^x = QK_1^x \le H$. 完成证明. □

关于幂零子群另一个深刻的结果是：

定理 3.8 (Wielandt) 两个幂零群之积可解.

这个定理的证明太长，有兴趣的读者可参阅 Huppert 的 *Endliche Gruppen I*, VI, §4. Казарин 于 1979 年证明了下述久而未决的 Scott 猜想：若 $G = AB$, 子群 A, B 均有一个指数 ≤ 2 的幂零子群，则 G 可解. 这是定理 3.8 的进一步推广. 见上册参考文献 [51].

习 题

1. (Carter) 如果一个幂零子群自正规化，这个子群就叫做 Carter 子群. 证明可解群必有 Carter 子群且所有 Carter 子群彼此共轭.

2. (郭秀云) 若群 G 的每个有合数指数的极大子群为幂零，则 G 为可解.

3. (Rose) 设非可解群 G 有一个幂零极大子群 H. 令 U 为 H 的正规 2-补. 证明 $U \lhd G$.

4. (Itô) 设 $G = AB$, A 与 B 为交换群，证明 $G'' = 1$. 特别地，G 是可解群.

§4. Deskins 的指数复合

由极大子群研讨群的结构是一个常用的并且是有效的方法. Deskins 的指数复合和下一节要介绍的正规指数提供了研究极大子群的新途径.

定义 4.1 设 M 是 G 的一个极大子群. G 的一个子群 C 称为 M 在 G 中的一个完备, 如果 $C \not\subseteq M$, 而 C 的每个 G-不变真子群都在 M 中. 用 $K(C)$ 表示 C 的所有 G-不变真子群之积, 则 $K(C) < C$ 且 $K(C) \lhd G$. M 在 G 中的所有完备作成一个集合, 记为 $I(M)$, 叫做 M 在 G 中的 指数复合. $I(M)$ 接集合包含关系作成一个偏序集, 其极大元称为 M 的 极大完备.

很容易证明, 对每个极大子群 $M, I(M)$ 是非空的. 因为总存在 $U \trianglelefteq G$ 使得 $G = MU$. 在这些 U 中取最小者, 则它就是 M 的一个完备. 显然地, 如果 $C \in I(M)$, 并且 $C \trianglelefteq G$, 那么 C 一定是一个极大完备.

定义 4.2 群 X 称为群 Y 的一个截断, 如果 X 是 Y 的一个子群的同态像

下面的引理对于讨论极大完备十分有用.

引理 4.3 令 G 是一个群, $N \lhd G$ 使得 G/N 有唯一极小正规子群 U/N. 令 M 是 G 的一个极大子群满足: M 包含 N, 但不包含 U. 并且令 C 是 $I(M)$ 的一个极大元. 进一步假设 U/N 不是 $C/K(C)$ 的截断, 那么

(1) $N = K(C)$, 且

(2) C 是 UC 的极大子群.

证 因 $K(C) \subseteq \mathrm{Core}_G(M)$, 且引理的假设蕴含 $N = \mathrm{Core}_G(M)$, 我们有 $K(C) \leq N$. 如果 $K(C) < N$, 则 $N \not\subseteq C$, 且 $CN > C$. 由于 C 为 $I(M)$ 的极大元, 故 $CN \notin I(M)$. 于是 $\mathrm{Core}_G(CN) \not\subseteq M$. 但是 $N \leq M$ 且 $N = \mathrm{Core}_G(M)$, 所以 $N < \mathrm{Core}_G(CN)$. 从而由 U/N 为 G/N 的唯一极小正规子群推出

$U \subseteq CN$. 这意味着 U/N 是 $C/K(C)$ 的一个截断, 矛盾于假设. 这证明了 (1).

如果 $U \subseteq C$ 那么 U/N 是 C/N 的一个子群, 当然 U/N 是 $C/K(C) = C/N$ 的一个截断, 矛盾于假设. 所以 $C < UC$. 设 B 是 UC 的一个子群使得 $C < B \leq UC$. 像 (1) 的证明一样, 我们有 $B \notin I(M)$, 且 $N \subseteq \mathrm{Core}_G(B) \not\subseteq M$, 得出 $U \subseteq \mathrm{Core}_G(B)$. 于是 $B = UC$, 即 C 为 UC 的极大子群. (2) 获证. □

定理 4.4 (Deskins) *群 G 可解当且仅当对于 G 的每个极大子群 M, 存在 $I(M)$ 的极大元 C 使得 $C/K(C)$ 是幂零的, 其 Sylow 2-子群的幂零类 ≤ 2.*

证 必要性容易证明, 因为 G 可解, 故 G 的主因子皆为交换群. 在非空集合 $\{U \mid U \trianglelefteq G$ 且 $G = UM\}$ 中取极小者 C, 则 C 为 M 的一个极大完备, 且 $C/K(C)$ 是 G 的一个主因子, 因而为交换群.

充分性. 设 G 是一个极小反例. 选取 $N \triangleleft G$ 尽可能大使得 G/N 非可解. 那么 G/N 有唯一个极小正规子群 U/N, 并且 U/N 非可解. 于是存在 G 的极大子群 M 满足: M 包含 N 但不包含 U. 由假设 $I(M)$ 有极大元 C 使得 $C/K(C)$ 是幂零的, 其 Sylow 2-子群的幂零类 ≤ 2. 显然 U/N 不是 $C/K(C)$ 的截断. 由引理 4.3 知 C 是 UC 的极大子群, 且 $N = K(C)$. 于是 C/N 是 UC/N 的极大子群, 其 Sylow 2-子群的幂零类 ≤ 2. 由定理 3.5 得 UC/N 可解, 于是 U/N 当然可解, 这是一个矛盾. 充分性证毕. □

定理 4.4 中条件“幂零类 ≤ 2 ”不能取消. 例如取 $G = PGL(2,17)$, 则 G 的 Sylow 2-子群是极大子群. $\mathrm{Soc}(G) = PSL(2,17)$ 是 G 的一个极大子群, 其指数为 2, 它有唯一个极大完备, 这就是 G 自身, 而 $G/K(G)$ 是一个 2 阶循环群. G 的其它极大子群是无核的, 它们都有一个极大完备为 G 的 Sylow 2-子群 P, 而 $P/K(P)$ 当然是幂零的, 但是 G 非可解.

Ballester-Bolinches 和郭秀云曾证明: 群 G 是可解的当且仅当对于 G 的每个极大子群 M, 存在一个极大元 $C \in I(M)$ 使得

$C/K(C)$ 幂零，且 $G=CM$. 一个改进了的结果是：

定理 4.5 *群 G 是可解的当且仅当对于 G 的每个有合数指数的极大子群 M, $I(M)$ 包含一个极大元 C 使得 $C/K(C)$ 是幂零的，并且 $C^g \not\subseteq M$ 对一切 $g \in G$ 成立.*

证 必要性见定理 4.4. 我们来证明充分性. 假设 G 是非可解的，并且 G 是一个极小阶反例. 选取 $N \lhd G$ 具有尽可能大的阶使得 G/N 非可解. 那么 G/N 有唯一个极小正规子群 U/N, U/N 非可解.

记 $\overline{G}=G/N, \overline{U}=U/N$. 令 q 为 $|\overline{U}|$ 的最大素因子， $\overline{Q} \in \mathrm{Syl}_q(\overline{U})$. 那么 $\overline{Q}$ 在 $\overline{U}$ 中非正规，所以存在 G 的极大子群 H 使得 $N_{\overline{G}}(\overline{Q}) \subseteq \overline{H}$. 由引理 1.11 知 $|\overline{G}:\overline{H}|$ 是合数, 所以 H 有合数指数. 现在我们取定 G 的一个有合数指数的极大子群, 仍以 H 表示. 由假设，$I(H)$ 包含一个极大元 C 使得 $C^g \not\subseteq H$ 对一切 $g \in G$ 成立, 且 $C/K(C)$ 为幂零. 显然 U/N 不是 $C/K(C)$ 的截断, 故由引理 4.3 得 $N=K(C)$, 且 C 为 UC 的极大子群. 现在 UC/N 包含一个幂零极大子群 C/N, 由定理 3.5, C/N 是偶阶群. 又因为 U/N 是 G/N 的唯一极小正规子群且非可解，故 $C_G(U/N)=N$. 所以 UC/N 中不可能包含正规幂零子群，于是 C/N 必为 Hall 子群. 由定理 3.4 推出 C/N 是一个 2-群，特别地， $C \cap U/N$ 是 U/N 的 Sylow 2-子群. 记 $\overline{S}=S/N=C \cap U/N$. 由奇数阶群可解性定理，$N_{\overline{G}}(\overline{S})<\overline{G}$, 所以存在 G 的一个极大子群 M 使得 $N_{\overline{G}}(\overline{S}) \leq \overline{M}=M/N$, 并且 $C \leq M$. 由 Frattini 推理得 $G=MU$.

我们来证明 $C=M$. 否则， $C<M$. 因为 C 是 $I(H)$ 的极大元，故 $\mathrm{Core}_G(M) \not\subseteq H$, 于是 $N<\mathrm{Core}_G(M)$. 由于 U/N 是 G/N 的唯一极小正规子群，必有 $U \subseteq \mathrm{Core}_G(M)$, 得出 $MU=M<G$, 矛盾. $C=M$ 得证. 这样， C/N 是 G/N 的幂零极大子群. 但是前证 C/N 是一个 2-群，并且 G/N 非可解，所以 $|G:C|$ 是合数. 于是我们可以用 C 代 H, 即假设 $N \leq H$ 并且 H/N 是 G/N 的一个 Sylow 2-子群. 这样一来， $C^g \not\subseteq H$ 不可能对一切 $g \in G$ 成立. 这是一个矛盾，完成证明. □

Deskins 猜测, 一个群 G 是超可解的当且仅当对于 G 的每个极大子群 M, $I(M)$ 有一个极大元 C 使得 $C/K(C)$ 是循环群, 且 $G = CM$. Ballester-Bolinches 指出这个猜测是否定的. 反例有 S_4(四个文字上的对称群). 稍后, 赵耀庆给出 Deskins 猜想的一个完整回答: 在上述条件下, G 或为超可解或者 G 有一个同态像与 S_4 同构.

定理 4.6 *群 G 是超可解的当且仅当对于 G 的每个有合数指数的极大子群 M, $I(M)$ 包含一个极大元 C 使得 $|C/K(C)|$ 无平方因子, 且 $G = CM$.*

在证明定理 4.6 之前, 先证明几个引理

引理 4.7 *设群 $G = CD$, 子群 C 与 D 的阶无平方因子. 那么 G 是可解的.*

证 假设 G 是非可解的. 由 Feit-Thompson 定理, G 不是 2-幂零的. 于是 $|G|_2 = 4$, 所以 $|C|$ 与 $|D|$ 都是偶数, 而 $|C \cap D|$ 为奇数. 令 $T \in \mathrm{Syl}_2(G)$, 则 T 是 4 阶初等交换群. 因为 G 不是 2-幂零的, 由 Burnside 定理 (上册 II, 定理 5.4), $T \not\subseteq N_G(T)$, 故存在一个奇阶元非平凡作用在 T 上, 并且置换 T 的对合, 从而 G 的所有对合共轭. 现在选择对合 $s \in C, t \in D$, 那么存在 $g \in G$ 使 $s^g = t$. 记 $g = cd$, 这里 $c \in C$, 而 $d \in D$, 则有 $s^{cd} = t$, 从而 $s^c = t^{d^{-1}}$ 是 $C \cap D$ 的一个对合. 这是一个矛盾, 完成证明. □

引理 4.8 *令 $M \leq G$, $|M|$ 无平方因子且有素数指数, 则 G 为可解.*

证 我们有 $G = MP$, 这里 $P \in \mathrm{Syl}_p(G)$, 而 p 是一个素数. 令 $B = M \cap P$, 则 B 在 P 中有指数 p. 因此 $B^G = B^{PM} = B^M \leq \mathrm{Core}_G(M)$, 所以 $G/\mathrm{Core}_G(M)$ 与 $\mathrm{Core}_G(M)$ 的阶均无平方因子, 所以 G 为可解. □

引理 4.9 *设 M 是群 G 的一个可解极大子群, K 是 G 的非可解正规子群使得 $G = MK$, 那么 $M \cap K > 1$.*

证 对 $|G|$ 用归纳法. 记 $M_G = \mathrm{Core}_G(M)$. 如果 $M_G > 1$, 则 $(M/M_G) \cap (M_G K/M_G) > 1$, 这意味着 $M \cap M_G K = (M \cap K)M_G > M_G$, 所以 $M \cap K > 1$, 引理已成立. 故可设 $M_G = 1$.

因 M 可解, M 有正规 p-子群 $P > 1$, p 为某个素数. 由第 VII 章定理 1.9 知 K 中存在 P-不变 Sylow p-子群 S. 若 $S > 1$, 则 $N_S(P) > 1$. 但是 $N_G(P) = M$(因为 $M_G = 1$), 所以 $M \cap K \geq M \cap S > 1$, 引理已成立. 于是又可设 K 为 p'-群. 现在 p-群 P 作用在 p'-群 K 上, 由第 VII 章引理 3.1 知对任一素数 $q \mid |K|$, K 有唯一 P-不变 Sylow q-子群 Q. 任取 $m \in M$ 及 $x \in P$, 我们有

$$(Q^m)^x = Q^{mxm^{-1}m} = (Q^{mxm^{-1}})^m = Q^m.$$

所以对每个 $m \in M, Q^m$ 也是 P-不变 Sylow q-子群. 由 Q 的唯一性得 $Q^m = Q$. 于是 Q 是 M-不变的, 从而 $G = MQ$. 这样一来, $K = Q$ 为可解. 这是一个矛盾, 完成证明. □

定理 4.6 的证明: 假设 G 是超可解的, 那么 G 的每个极大子群 M 有素数指数, 故关于 $I(M)$ 的条件自动成立.

证充分性. 首先证明 G 是可解的. 用反证法. 设 G 非可解, 选取 $N \lhd G$ 使得 G/N 非可解, 并且 N 有尽可能大的阶. 那么 G/N 有唯一个极小正规子群 U/N, 且 U/N 非可解. 当然, U/N 不含非平凡正规素数幂阶子群. 令 p 是 $|U/N|$ 的最大素因子, $P/N \in \mathrm{Syl}_p(U/N)$. 那么 P 在 U 中非正规, 故存在 G 的极大子群 M 包含 $N_G(P)$ 而不包含 U. 由引理 1.11, M 有合数指数.

现在可以假设 M 是 G 的任一个具有合数指数的极大子群能使 M 包含 N 而不包含 U. 由假设 $I(M)$ 包含一个极大元 C 使得 $|C/K(C)|$ 无平方因子. 当然 $C/K(C)$ 可解, 故 U/N 不是 $C/K(C)$ 的截断, 由引理 4.3, $N = K(C)$, 且 C 是 UC 的极大子群. 记 $E = CU, T = C \cap U$. 那么 T/N 是 U/N 的极大 C/N-不变真子群, 而 U/N 是 E/N 的非可解正规子群, 由引理 4.9 得 $T/N > 1$. 又因为 T/N 是 C/N 的子群, 所以 $|T/N|$ 无平方因子, 于是 T/N 有一个非平凡正规 Sylow q-子群 Q/N, q 为某个素数. 因为 $T/N \lhd C/N$, 我们有 $Q \lhd C$ 且 $C \subseteq N_G(Q)$. 前面说

过，U/N 没有非平凡的素数幂阶正规子群，故 $U \not\subseteq N_G(Q)$. 但是，U/N 是 G/N 的唯一极小正规子群，于是知 $N_G(Q)/N$ 是无核的，推出 $N_G(Q) \in I(M)$. 由 C 的极大性得 $C = N_G(Q)$. 又因 $T \le N_U(Q) = U \cap N_G(Q) = U \cap C = T$, 得出 $T = N_U(Q)$.

现在 $T/N = N_U(Q)/N = N_{U/N}(Q/N)$, 得知 Q/N 是 U/N 的 Sylow q-子群. 由 Frattini 论断，$G = UN_G(Q) = UC$, 推出 $E = G$, 故 C 为 G 的极大子群. 由假设，$|C/K(C)|$ 无平方因子，又 G 非可解，由引理 4.8, C 是 G 的合数指数极大子群. 我们可以 C 代 M, 即假设 $|M|$ 无平方因子. 于是 $G = CM$ 中 C/N 与 M/N 的阶均无平方因子, 由引理 4.7 得 G/N 为可解. 完成 G 可解的证明.

现在我们很容易证明 G 是超可解群. 因为 G 可解，所以 G 的每个极大子群的指数为素数幂. 假如 G 有指数为合数的极大子群 M, 由假设 $I(M)$ 包含一个极大之 C 使 $|C/K(C)|$ 无平方因子，且 $G = MC$. 由此推出 $|G : M|$ 无平方因子，于是 M 有素数指数，这是一个矛盾. 因此 G 的每个极大子群均有素数指数，由定理 1.12 得 G 为超可解.

定理 4.10 令 G 是一个群. 假设对于 G 的每个合数指数极大子群 $M, I(M)$ 包含一个极大元 C 使得 $C/K(C)$ 循环，其阶大于或等于 $|G : M|$. 那么 G 是可解的，且下述结论成立:

(1) G 的每个极大子群的指数或为素数或为 4.

(2) 若 G 非超可解，则 G 有一个同态像与 S_4 同构.

证 由定理 4.4, G 是可解的. 假设 G 非超可解. 令 M 是 G 的一个合数指数极大子群, 我们要证 $|G : M| = 4$. 令 $N = \mathrm{Core}_G(M)$, U/N 是 G 的一个主因子, 那么 U/N 是非循环初等交换 p-群, 而 p 为适当的素数，$G = UM$ 且 $U \cap M = N$. 我们还有 $C_M(U/N) \lhd G$, 故得 $C_M(U/N) = N$, 从而 $C_G(U/N) = U$. 由此推出 U/N 是 G/N 的唯一极小正规子群. 因为 $|G : M| = |U : N|$, 我们只需证 $|U/N| = 4$.

由假设，$I(M)$ 包含一个极大元 C 使得 $C/K(C)$ 循环且 $|C/K(C)| \ge |G : M|$. 因为 U/N 非循环，故 U/N 不是 $C/K(C)$ 的截断，应用引理 4.3 我们有 $K(C) = N$, 且 C 是 $E = UC$ 的

极大子群. 同时, $|C/N| \geq |G:M|$, 故 $|C| \geq |U|$. 我们能够断言 $C \triangleleft E$. 假设不真, 则 E/N 不能是 p-群, 从而 C/N 也不是 p-群, 于是 $|C/N| \neq |U/N|$, 推出 $|C| > |U|$. 令 B 是 C 在 E 中的一个共轭, 且 $B \neq C$, 那么 $|B \cap C| > |U \cap C|$. 由此推出 $B \cap C \not\subseteq U$, 于是, 因为 $C_G(U/N) = U$, 我们知 $B \cap C$ 不中心化 U/N. 令 $X/N = C_{G/N}(B \cap C)$. 则 $U \not\subseteq X$, 故 X/N 是无核的, 于是 $X \in I(M)$. 但是 B/N 和 C/N 都是交换群, 故知 X 包含 B 和 C. 由 C 的极大性得 $B \leq X = C$, 与 B 的定义矛盾. 这证明了断言.

令 $T = U \cap C$. 现在 C 是 E 的极大子群且正规, 所以 $|U:T| = |E:C|$ 是一个素数, 因此这个数为 p, 且 E/N 是一个 p-群. 因为 T/N 是 U/N 的非平凡循环子群, 而 U/N 是初等交换 p-群, 所以 T/N 为 p 阶循环群, 从而得 $|U:N| = p^2$. 剩下要证的是 $p = 2$.

我们有 $|C| \geq |U| > |T|$, 故 $E > U$. 令 V 是 E 的一个子群使得 V 包含 U, 并且 $|V:U| = p$. 那么 $V \cap C > T$, 且 $V \cap C/N$ 循环. 于是 V/N 是 p^3 阶群, 其方次数为 p^2. 令 $Q = V \cap M$. 则 Q/N 是 V/N 的 p 阶子群且 $Q/N \not\subseteq U/N$. 故 V/N 的 p 阶元至少有 p^2 个. 如果 $p > 2$, 有此性质的 p^3 阶群必定有方次数 p, 一个矛盾. 于是 $p = 2$.

最后, 证明 $G/N \cong S_4$. 因为 U/N 是 4 阶初等交换 2-群, 考虑 G/N 关于 M/N 的 4 个陪集上的置换表示, 立得结论, 完成证明.

习 题

1. 证明 S_4 的每个极大子群 M 有一个极大完备 C 使得 $C/K(C)$ 是循环群, 且 $S_4 = MC$.

2. 假设群 G 的每个极大子群 M 有一个极大完备 C 使得 $C/K(C)$ 是素数阶群. G 一定超可解吗?

3. (赵耀庆) 设 G 为可解群. 如果对于 G 的每个极大子群 M, $I(M)$ 包含一个元 C (不必极大) 使得 $G = CM$ 并且 $C/K(C)$ 是循环群, 那么或

者 G 为超可解，或者 G 有一个同态像与 S_4 同构.

4. (赵耀庆) 群 G 是可解的当且仅当 G 有一个可解极大子群 M, 并且 $I(M)$ 有一个极大元 C 使得 $C/K(C)$ 幂零，其 Sylow 2-子群的幂零类 ≤ 2.

§5. 正规指数

正规指数的概念由 Deskins 于 1959 年提出. 他给出正规指数的第一个结果：一个群是可解的当且当仅当它的每个极大子群的正规指数等于其指数. 但是，关于正规指数较为系统的结果是近十年来获得的. 正规指数着重用算术条件来刻画群的结构，这是正规指数的特色.

定义 5.1 给了群 G 及极大子群 M. 令 N/K 是 G 的一个主因子，满足 $G=MN$ 并且 N 有尽可能小的阶. N/K 的阶叫做 M 在 G 中的 *正规指数*, 记作 $\eta(G:M)$.

当然，我们需要证明 $\eta(G:M)$ 是唯一确定的. 但是这件事暂且放下，让我们来考虑另一个问题.

定义 5.2 给定群 G 及 G 的极大子群 M. 令 N/K 是 G 的一个主因子， $K\leq M$ 而 $N\not\subseteq M$. 称 $M\cap N/K$ 为 M 的一个 CI-截.

命题 5.3 *对于 G 的任一极大子群 M, M 的 CI-截在同构意义下唯一.*

为了证明这个性质，需要 *本原群* 的一个结果.

定义 5.4 群 G 叫做本原的，如果它有一个极大子群 M 使得 $\mathrm{Core}_G(M)=1$, M 叫做 G 的一个稳定子.

定理 5.5 (Baer) *令 G 是一个本原群， M 为稳定子. 那么下述结论之一成立.*

(1) G 有唯一个极小正规子群 N, N 自中心化 (当然 N 为交换).

(2) G 有唯一个极小正规子群 N, N 非交换.

(3) G 恰好有两个极小正规子群 N 和 N^*, $C_G(N) = N^*$, $C_G(N^*) = N$ 且 $N \cong N^* \cong NN^* \cap M$. 还有, 如果 $V < G, VN = VN^* = G$, 那么 $V \cap N = V \cap N^*=1$.

证 令 $1 \neq K \trianglelefteq G, C = C_G(K)$. 因 $K \not\subseteq M$, 我们有

$$KM = G.$$

又因 $C \triangleleft G$, 有 $C \cap M \triangleleft M$ 并且 K 中心化 $C \cap M$, 所以 $C \cap M \triangleleft MK = G$. 因此

$$C \cap M = 1.$$

如果 $D \trianglelefteq G$ 使得 $1 \neq D \leq C$, 那么 $C = C \cap DM = D(C \cap M) = D$. 因此

(i) $C=1$ 或者

(ii) C 是 G 的极小正规子群.

下分三种情形讨论:

(1) G 有一个交换正规子群 $N \neq 1$. 取 $K = N$. 那么 $N \leq C = C_G(N)$, 于是由 (ii) 得 $N = C_G(N)$, 从而 N 是 G 的唯一极小正规子群.

(2) G 有唯一个极小正规子群 N 且 N 非交换.

(3) G 至少有两个极小正规子群 N 和 N^*. 取 $K = N$. 设 N^{**} 是 G 的第三个极小正规子群, 那么 $N^*N^{**} \leq C = C_G(N)$, 与 (i)-(ii) 矛盾. 因此 G 恰有两个极小正规子群 N, N^*. 因为 $N^* \leq C$, 由 (ii) 推出 $C_G(N) = N^*$, 同理又有 $C_G(N^*) = N$.

其次, $N(NN^* \cap M) = NN^* \cap NM = NN^*$, 所以

$$N^* \cong NN^*/N = N(NN^* \cap M)/N \cong NN^* \cap M.$$

类似地 $N \cong N^*N \cap M$, 所以 $N^* \cong N$. 最后, 若 $V < G$ 使得 $VN = VN^* = G$, 那么 $V \cap N \triangleleft \langle V, N^* \rangle = G$, 推出 $V \cap N=1$. 同理, $V \cap N^* = 1$. 证毕. □

命题 5.3 的证明 令 M 是群 G 的一个极大子群, N/K 是 G 的一个主因子使得 $K \le M$ 而 $N \not\le M$. 由定义 $N \cap M/K$ 是 M 的一个 CI-截. 令 $M_G = \mathrm{Core}_G(M), U = NM_G$, 则 $K \le M_G$, 且 U/M_G 也是 G 的一个主因子, 而且 $U/M_G \cong N/K$. 现在 G/M_G 是一个本原群, 以 M/M_G 为稳定子. 如果 U/M_G 是 G/M_G 的唯一极小正规子群, 结论显然成立. 否则, 由定理 5.5, G/M_G 恰有两个极小正规子群 U/M_G 和 V/M_G, $U/M_G \cong V/M_G$ 并且 $U \cap M = M_G = V \cap M$. 所以 $V \cap M/M_G = U \cap M/M_G = NM_G \cap M/M_G = (N \cap M)M_G/M_G \cong N \cap M/N \cap M \cap M_G = N \cap M/N \cap M_G = N \cap M/K$. 完成证明.
□

命题 5.6 令 $N \le M < G$, M 是 G 的极大子群, $N \lhd G$. 那么 M 与 M/N 有同构的 CI-截.

证 这是命题 5.3 的直接推论. □

命题 5.7 令 M 是群 G 的一个极大子群, $\sigma(M)$ 表示 M 的 CI-截. 那么

$$\eta(G:M) = |\sigma(M)||G:M|.$$

特别地 $\eta(G:M)$ 由 M 唯一确定.

证 令 N/K 是 G 的一个主因子使得 $G = NM$, 并且 N 有尽可能小的阶. 由定义 5.1, $\eta(G:M) = |N/K|$. 由 N 的极小性, 有 $K \le M$. 于是 $N \cap M/K$ 是 M 的一个 CI-截, 故 $\eta(G:M) = |N:M \cap N||M \cap N:K| = |G:M||\sigma(M)|$. □

为了叙述方便, 我们用 $\mathcal{F}$ 表示 G 的极大子群的集合并定义

$$\begin{aligned}
\mathcal{F}_{pc} = \quad & \{M \mid \quad M \in \mathcal{F}, |G:M|_p = 1 \text{ 且 } |G:M| \text{ 是合数}\},\\
\mathcal{F}^{pc} = \quad & \{M \mid \quad M \in \mathcal{F}, |G:M| \text{ 是合数且 } M \text{ 包含 G 的一}\\
& \qquad\qquad \text{个 Sylow}p\text{-子群的正规化子}\}.
\end{aligned}$$

CI-截对于讨论正规指数有一定的价值, 所以我们先来研究 CI-截对群结构的影响.

设 P 是一个素数幂阶群，用 $J(P)$ 表示 P 的 Thompson 子群 (见第 VIII 章，定义 4.6). 首先，我们叙述一个有用的定理，其证明见 Petter 的文章： A note on finite groups having a fixed-point-free automorphism, *Proc. Amer. Math. Soc.*, 52(1975), 79–80.

命题 5.8 (Petter). *群 G 是 2-闭的 (即 Sylow 2-子群正规) 当且仅当对于 G 的每个奇阶 Sylow 子群 P, $N_G(Z(J(P)))$ 是 2-闭的.*

定理 5.9 *群 G 是可解的当且仅当它的每个极大子群的 CI-截是 2-闭的.*

证 假设 G 的每个极大子群的 CI-截是 2-闭的，我们来证明 G 是可解群. 令 N 是 G 的一个极小正规子群. 由命题 5.6, G/N 满足定理的假设，归纳得 G/N 为可解，由此又知 N 为 G 的唯一极小正规子群. 因此只需证明 N 为可解. 假设 N 非可解. 令 P 为 N 的任一奇阶 Sylow 子群. 由 Frattini 推理得 $G = N_G(P)N = N_G(Z(J(P)))N$. 当然 $N_G(Z(J(P))) < G$, 故 G 有极大子群 M 包含 $N_G(Z(J(P)))$, 但是 $N \not\subseteq M$. 由 N 的唯一性又得 $\mathrm{Core}_G(M)=1$. 从而 $M \cap N$ 为 M 的 CI-截. 由假设它是 2-闭的，而 $N_N(Z(J(P))) \leq M \cap N$, 故亦为 2-闭. 应用命题 5.8, N 是 2-闭的，于是由奇阶群可解定理推出 N 为可解. 这是一个矛盾.

反过来，对于 G 的每个极大子群 M, 因为假设 G 可解， G 有主因子 $K/\mathrm{Core}_G(M)$ 为素数幂阶群，且 $M \cap K = \mathrm{Core}_G(M)$, 故 M 有平凡的 CI-截，当然为 2-闭. □

定理 5.10 *群 G 是可解的当且仅当对于 G 的每个极大子群 $M \in \mathcal{F}_{pc}$, M 的 CI-截为幂零，这里 p 是 $|G|$ 的最大素因子.*

证 必要性见定理 5.9. 下面证充分性. 令 G 是一个极小阶反例. 考虑 G 的一个极小正规子群 N. 由命题 5.6, G/N 满足定理的假设，由 G 的极小性知 G/N 为可解，从而又可推出 N 为 G 的唯一极小正规子群，并且 N 非可解. 令 q 为 $|N|$ 的最大素因子， $Q \in \mathrm{Syl}_q(N)$. 那么 Q 在 N 中非正规，且 $q > 2$. 由引理 1.11, G 存在极大子群 M 包含 $N_G(Z(J(Q)))$, 且 $|G : M|$

为合数. 由 Frattini 论断得 $G = MN$, 可见 M 包含 G 的一个 Sylow p-子群, 所以 $M \in \mathcal{F}_{pc}$. N 的唯一性推出 $\mathrm{Core}_G(M)=1$. 于是 $M \cap N$ 是 M 的一个 CI-截, 由假设 $M \cap N$ 为幂零. 但是 $N_N(Z(J(Q))) = N \cap N_G(Z(J(Q))) \leq N \cap M$, 所以 $N_N(Z(J(Q)))$ 为幂零. 由第 VIII 章定理 5.1, N 为 q-幂零. 这当然不可能. 完成证明. □

接下来讨论群的 π-可解性.

定理 5.11 *令 G 是群, p 是 $|G|$ 的最大素因子. 那么 G 是 p-可解的当且仅当对 G 的每个极大子群 $M \in \mathcal{F}^{pc}$, M 的 CI-截是 p-幂零的.*

证 先证充分性. 对 $|G|$ 用归纳法. 令 P 是 G 的 Sylow p-子群. 如果 $P \lhd G$, 那么 G 当然是 p-可解的. 所以假设 $N_G(P) < G$. 令 N 是 G 的极小正规子群. 我们能够断言, G/N 为 p-可解. 事实上, PN/N 是 G/N 的一个 Sylow p-子群, 且 $N_G(P)N/N \leq N_{G/N}(PN/N)$. 令 M/N 是 G/N 的有合数指数的极大子群使得 $N_{G/N}(PN/N) \leq M/N$, 那么 $M \in \mathcal{F}^{pc}$. 由假设, M 的 CI-截为 p-幂零, 所以 M/N 的 CI-截也是 p-幂零. 这意味着 G/N 满足定理的条件, 由归纳得 G/N 为 p-可解. 我们还可以假设 N 是 G 的唯一极小正规子群.

我们来证明 N 为 p-可解. 否则, p 是 $|N|$ 的最大素因子, $P_0 = P \cap N > 1$ 是 N 的 Sylow p-子群, 并且 $N_G(P) \leq N_G(P_0) \leq N_G(Z(J(P_0))) \leq M$, 而 M 是 G 的一个极大子群. 由引理 1.11, M 有合数指数, 故 $M \in \mathcal{F}^{pc}$. 由 Frattini 论断还有 $G = MN$. 接下来由 N 的唯一性得 $\mathrm{Core}_G(M) = 1$, 所以 $M \cap N$ 是 M 的一个 CI-截. 由假设, $M \cap N$ 为 p-幂零, 当然, $N_N(Z(J(P_0)))$ 作为 $M \cap N$ 的子群也是 p-幂零. 注意到 $p > 2$, 由第 VIII 章定理 5.1, N 为 p-幂零, 这不可能. 这样, G/N 与 N 均为 p-可解, 从而 G 为 p-可解.

条件的必要性容易证明. 因为 G 为 p-可解, G 的每个主因子或为 p-群或为 p'-群. 令 M 为 G 的任一极大子群, 取 G 的主因

子 $N/\mathrm{Core}_G(M)$, 那么 $N\cap M/\mathrm{Core}_G(M)$ 或为 p-群或为 p'-群，当然是 p-幂零. 证毕. □

定理 5.12 *群 G 是 π-可解的当且仅当对于 G 的每个非幂零极大子群 M, M 的 CI-截为 π'-群.*

证 必要性的证明类似定理 5.11. 我们来证明充分性. 令 G 是一个极小阶反例，N 为 G 的一个极小正规子群. 那么 G/N 是 π-可解的，并且 N 是 G 的唯一极小正规子群.

如果 N 是 π'-群, 那么 G/N 和 N 都是 π-可解的, 从而 G 为 π-可解, 矛盾于 G 为反例. 于是可设 N 不是 π'-群. 令 $\pi_1=\{p\bigm| p\in\pi$ 且 $p\bigm| |N|\}$. 那么 π_1 是非空的. 对于任一取定的 $p\in\pi_1$, 令 P 是 N 的一个 Sylow p-子群. 我们有 $1<N_G(P)\le N_G(Z(J(P)))<G$. 所以存在 G 的极大子群 $M\supseteq N_G(Z(J(P)))$, 并且应用 Frattini 论断得 $G=MN$. N 的唯一性又推出 $\mathrm{Core}_G(M)=1$, 所以 $M\cap N$ 是 M 的一个 CI-截. 假若 M 是非幂零的, 由假设 $M\cap N$ 为 π'-群, 矛盾于 $M\cap N$ 包含一个 π-子群 P. 所以 M 是幂零的, 从而 $N_N(Z(J(P)))$ 为幂零. 因为 N 不可能是 p-幂零的，由第 VIII 章定理 5.1 得出 $p=2$. 于是由 p 的任意性得 $\pi_1=\{2\}$. 这样，$2\notin\pi'$.

令 q 是 $|N|$ 的任一奇素因子，$Q\in\mathrm{Syl}_q(N)$. 由上一段的证明知，G 有非幂零极大子群 H 使得 $N_G(Z(J(Q)))\le H$ 且 $\mathrm{Core}_G(H)=1$. 由假设 CI-截 $H\cap N$ 为 π'-群. 特别地 $N_N(Z(J(Q)))$ 是奇阶群. 应用命题 5.8 得 N 为 2-闭群，再由 N 的极小性得 N 为 2-群. 现在 G/N 和 N 均为 π-可解，从而 G 为 π-可解，矛盾于 G 为反例. 证毕. □

由前面关于 CI-截的定理及命题 5.7, 立得一系列关于正规指数的结果.

定理 5.13 *给了一个群 G, 则下述命题两两等价:*

(1) G 是可解的.

(2) 对于 G 的每个极大子群 M, $\eta(G:M)/|G:M|$ 是一个素数幂或为奇数.

(3) 对于 G 的每个极大子群 $M \in \mathcal{F}_{pc}$, $\eta(G:M)/|G:M|$ 是一个素数幂, 这里 p 为 $|G|$ 的最大素因子.

证 由定理 5.9, 定理 5.10 及命题 5.7 推出. □

推论 5.14 (Deskins) 群 G 是可解的当且仅当对 G 的每个极大子群 M, $\eta(G:M) = |G:M|$.

定理 5.15 群 G 是 p-可解的当且仅当对于 G 的每个极大子群 $M \in \mathcal{F}^{pc}$, $\eta(G:M)/|G:M|$ 是 p 的幂或 p'-数, 这里 p 是 $|G|$ 的最大素因子.

证 由定理 5.11 及命题 5.7 推出. □

定理 5.16 群 G 是 π-可解的当且仅当对 G 的每个非幂零极大子群 M, $\eta(G:M)/|G:M|$ 是 π'-数.

证 由定理 5.12 及命题 5.7 推出. □

现在我们来特征超可解群和 π-超可解群.

定理 5.17 (Ballester-Bolinches) 群 G 是 π-超可解的当且仅当对于 G 的每个有合数指数的极大子群 M, $\eta(G:M)_\pi=1$.

证 设 G 为 π-超可解. 令 $N/\mathrm{Core}_G(M)$ 是一个主因子, 因为 $|G:M|$ 为合数, $N/\mathrm{Core}_G(M)$ 必须是 π-群, 于是 $\eta(G:M)_\pi=1$.

反过来, 假设 G 不是 π-超可解的, 并且 G 为极小阶反例. 令 N 为 G 的极小正规子群, 那么 G/N 是 π-超可解的, 由此又推出 N 是 G 的唯一极小正规子群. 如果 N 为 π'-群, 那么 G 为 π-超可解, 于是 N 不是 π'-群. 又若 $N \le \Phi(G)$, 同样推出 G 为 π-超可解. 因此 G 有极大子群 M 使得 $G = MN$ 且 $\mathrm{Core}_G(M) = 1$, 那么 $\eta(G:M) = |N|$ 不是 π'-数, 由假设 $|G:M|$ 是某个素数 p. 若 N 为交换, 则 N 为 p 阶循环群, 得出 G 为 π-超可解. 于是 N 为非交换. 令 q 为 $|N|$ 的最大素因子, $Q \in \mathrm{Syl}_q(N)$. 由引理 1.11, G 有合数指数的极大子群 H 使得 $N_G(Q) \le H$. 由 Frattini 推理

$G = HN$ 且 $\mathrm{Core}_G(H) = 1$, 再次得 $\eta(G:M) = |N|$ 不是 π'-数, 矛盾于假设. 证毕. □

类似的方法可证:

定理 5.18 (Makherjee-Bhatttaches) *群 G 是超可解的当且仅当对 G 的每个有合数指数的极大子群 M, $\eta(G:M)$ 无平方因子.*

习 题

1. 证明定理 5.18.

2. (郭秀云) 群 G 是超可解的当且仅当对 G 的每个极大子群 M, $\eta(G:M)$ 是素数.

3. (郭秀云) 如果群 G 有一个可解极大子群 M 能使 $\eta(G:M)$ 是奇数, 则 G 为可解.

4. (郭秀云) 如果群 G 有一个 p-可解极大子群 M 使得 $\eta(G:M)_{p'} = 1$, 则 G 为 p-可解.

5. (A. Ballester-Bolinches 和赵耀庆) 令 G 是 π-可解群, 则 G 可解当且仅当对 G 的每个满足 $|G:M|_\pi = 1$ 且有合数指数的极大子群 M, 恒有 $\eta(G:M)/|G:M|$ 是一个 π-数.

§6. 极小子群

极小子群, 即素数阶子群, 作为极大子群的对偶在有限群理论中扮演了一个重要的角色. 极小子群与正规条件结合起来, 常常能产生很强的结果.

首先, 我们叙述一个应用很广的经典性结果, 它可以从更一般形式的定理 6.2 推出.

定理 6.1 (Itô) *令 G 是一个群, 那么*

(1) 对于固定的奇素数 p, 假设 G 的一切 p 阶子群均包含在 $Z(G)$ 中, 则 G 为 p-幂零.

(2) 若 G 的 2 阶及 4 阶元均属于 $Z(G)$, 则 G 为 2-幂零.

定理 6.1 可以局部化为

定理 6.2 设 G 为群, p 是一个固定素数, P 是 G 的一个 Sylow p-子群. 假设 P 的每个 p 阶元属于 $Z(N_G(P))$. 若 p=2, 还假设 P 的每个 4 阶循环子群正规于 $N_G(P)$. 那么 G 是 p-幂零的.

证 令 G 是一个极小阶反例. 记 $N = N_G(P)$. 由 G 的极小性, G 的每个包含 N 的真子群为 p-幂零. 根据第 VIII 章定理 3.5 只需证明, 对于任意 $X \leq P$, M/C 是一个 p-群, 这里 $M = N_G(X)$, 而 $C = C_G(X)$.

令 $Y \leq X$ 是由 X 中一切 p 阶元及 4 阶元 (若 p=2) 生成的子群. 那么 Y 是 X 的特征子群, 故 $M \leq N_G(Y)$. 又由假设, $N_G(Y)$ 当然包含 $N_G(P)$. 若 $N_G(Y) < G$, 则 $N_G(Y)$ 为 p-幂零, 从而 M 为 p-幂零. 这样一来 M/C 为 p-群, 证明已完成. 于是可设 $Y \lhd G$.

现在定义子群 B 如下: 若 $p > 2$, 令 $B = C_G(Y)$, 若 p=2, 令 B 是 G 中这样的元素全体, 它中心化 Y 的每个 2 阶元, 也正规化 Y 的每个 4 阶循环子群. 不论哪种情形, B 的每个 p'-元平凡作用在 Y 上.

因为 $Y \lhd G$, 易知 $B \lhd G$. 由假设还有 $N \leq B$. 于是由 Frattini 推理, $B = G$. 这表明 G 的每个 p'-元平凡作用于 Y. 特别地, M 的任一 p'-元 m 中心化 Y. 由第 VII 章, 定理 3.4, m 中心化 X, 于是得 M/C 是一个 p-群. 证毕. □

当 p 为 $|G|$ 的最小素因子时, 定理 6.2 有一个更深刻的推广. 为此, 先介绍拟中心元.

定义 6.3 设 x 是群 G 的一个元. x 叫做 **拟中心的**, 如果 $\langle x\rangle\langle y\rangle = \langle y\rangle\langle x\rangle$ 对一切 $y \in G$ 成立.

命题 6.4 令 p 是 $|G|$ 的最小素因子. 若 x_1, x_2 是 G 的 p 阶拟中心元, 那么积 x_1x_2 仍为 G 的拟中心元, 且 $(x_1x_2)^p$=1.

证 记 $x = x_1x_2$. 显然有 x^p=1. 对于任意 $y \in G$ 成立着 $\langle x_i\rangle\langle y\rangle = \langle y\rangle\langle x_i\rangle, i = 1, 2$. 因为 p 是 $|G|$ 的最小素因子, 所以 x_i 正规化 $\langle y\rangle$, 于是 x 正规化 $\langle y\rangle$. 特别地 $\langle x\rangle\langle y\rangle = \langle y\rangle\langle x\rangle$. 证毕. □

命题 6.5 若 c 是 G 的一个 2 阶拟中心元, 那么 $\langle c\rangle$ 中心化 G 的 2 阶和 4 阶元.

证　任取 $x \in G$ 使得 $x^4=1$. 我们有 $\langle c\rangle\langle x\rangle = \langle x\rangle\langle c\rangle$. 假若 $[c,x]\neq 1$. 则 $c^{-1}xc = x^{-1}$, 所以 $(xc)^2=1$, 于是子群 $\langle c\rangle\langle x\rangle = \langle x\rangle\langle c\rangle$ 的阶 ≤ 4, 从而 $[c,x]=1$, 矛盾. □

命题 6.6 令 G 是一个 2-群. 假设 G 的每个 2 阶元是拟中心的. 那么 $\langle a\rangle/\langle c\rangle$ 中心化 $\Omega_1(G)/\langle c\rangle$, 这里 a 为 G 的任意元, 而 $c \in \langle a\rangle$ 是一个 2 阶元.

证　令 x 是 G 的任一 2 阶元. 那么对任意 $a \in G$, $\langle x\rangle\langle a\rangle$ 是 G 的子群. 因此 $x^{-1}ax = a^t, t^2 \equiv 1(\mathrm{mod}\ o(a) = 2^n)$, 并且 $(xa)^2 = xaxa = x^{-1}axa = a^{t+1}$. 如果 $4 \mid t+1$, 则 $o(xa) \mid 2^{n-1}$, 从而 $\langle x\rangle\langle xa\rangle = \langle x\rangle\langle a\rangle$ 的阶整除 2^n. 于是 $x \in \langle a\rangle$, 得出 $[a,x]=1$, 证明已完成. 因此设 $4 \nmid t+1$, 那么 $2^{n-1} \mid t-1$, 所以 $[a,x] = a^{t-1} \in \langle c\rangle$, 满足要求. □

现在我们能够证明

定理 6.7 令 G 是一个群, p 为 $|G|$ 的最小素因子, S 表示 G 的一个 Sylow p-子群. 假设下述条件成立:

(1) $\Omega_1(S)$ 由 $N_G(S)$ 的 p 阶拟中心元生成.

(2) 若 $p=2$, $\Omega_2(S)$ 由 $N_G(S)$ 的 2 阶和 4 阶拟中心元生成.

那么 G 是 p-幂零的.

证　假设定理不真, G 是一个极小阶反例. 证明中出现的 $\Omega_i(S)$ 及 $\Omega_i(X)$, 规定 $i=1$ 若 $p>2$, $i=2$ 若 $p=2$. 首先有

(1) $O_{p'}(G)=1$, 且 G 的每个包含 $N_G(S)$ 的真子群为 p-幂零.

令 χ 是一个子群集, 规定 $X \in \chi \Leftrightarrow 1 < X \leq S$ 使得 $N_G(X)$ 非 p-幂零, 但是 $N_G(V)$ 为 p-幂零只要 $X < V \leq S$.

(2) $\chi \neq \varnothing$, 且对每个 $X \in \chi$ 有 $1 < X < S$.

首先, 由第 III 章, 定理 4.3, $N_G(S) = S \rtimes C$, 这里 C 是 p'-群. 易知定理的假设蕴含 C 中心化 $\Omega_1(S)$, 若 $p=2$, C 还中心化 $\Omega_2(S)$.

于是由第 VII 章，定理 4.3 知，C 中心化 S, 故 $N_G(S)$ 为 p-幂零. 另一方面，因为 G 不是 p-幂零，由第 VIII 章，定理 3.5, 存在一个子群 $X \leq S$ 使得 $N_G(X)$ 不是 p-幂零的. 选取这样的 X 极大，那么 $1 < X < S$ 并且 $X \in \chi$.

(3) 对每个 $X \in \chi$, 总有 $\Omega_1(X) \lhd G$.

由命题 6.4, $\Omega_1(S)$ 是初等交换 p-群，因此 $N_G(\Omega_1(X))$ 包含 $\Omega_1(S)$ 和 $N_G(X)$. 若 $p=2$, 由命题 6.5 知 $\Omega_1(S) \leq Z(\Omega_2(S))$, 所以 $N_G(\Omega_1(X))$ 也包含 $\Omega_2(S)$. 记 $H = N_G(\Omega_1(X))$. 因 $N_G(X)$ 非 p-幂零，因而 H 也非 p-幂零. 令 S_0 是 H 的一个 Sylow p-子群使得 S_0 包含 $X\Omega_i(S)$. 因为 $X < S$, 我们有 $X < S_0$, 于是 $N_G(S_0)$ 为 p-幂零. 又显然有 $\Omega_i(S) = \Omega_i(S_0)$, 从而知 H 满足定理的条件，故得 $H = G$. 于是 $\Omega_1(X) \lhd G$.

(4) 若 p=2, 则 $\Omega_2(S)/\Omega_1(S)$ 的每个元在 $S/\Omega_1(S)$ 中是拟中心的.

由假设， $\Omega_2(S) = \langle x_1, \cdots, x_r\rangle$, 这里每个 x_i 是 S 的拟中心元，且 ${x_i}^4 = 1$. 所以，每个 $x_i\Omega_1(S)$ 是 $S/\Omega_1(S)$ 的拟中心元，阶为 2 或 1. 于是 (4) 由命题 6.4 推出.

(5) 存在一个 $X \in \chi$ 使得 $\Omega_1(S) \leq X$.

固定 $X \in \chi$. 令 $M = N_G(\Omega_i(X)), C = C_G(\Omega_i(X))\Omega_i(X)$. 我们有 $C \lhd M$ 且 $\Omega_1(S) \leq C$. 令 S_0 是 C 的一个 Sylow p-子群使得 S_0 包含 $\Omega_1(S)\Omega_i(X)$. 为了证明 (5), 我们只要证明 $N_G(S_0)$ 不是 p-幂零的. 因为在这种情形，我们可以选取尽可能大的 $Y \leq S$ 使得 Y 包含 S_0 并且 $N_G(Y)$ 不是 p-幂零的，那么 $Y \in \chi$ 而且满足要求.

现在假设 $N_G(S_0)$ 为 p-幂零. 当然， $N_M(S_0)$ 也是 p-幂零，于是它有一个正规 p-补 H, H 中心化 S_0, 特别地， H 中心化 $\Omega_i(X)$. 因而 $H \leq C_G(\Omega_i(X))$. 由 Frattini 论断

$$M = N_M(S_0)C = N_M(S_0)C_G(\Omega_i(X)).$$

从而

$$M/C_G(\Omega_i(X)) \cong N_M(S_0)/N_M(S_0) \cap C_G(\Omega_i(X))$$

是一个 p-群. 于是由 $N_G(X) \leq N_G(\Omega_i(X)) = M$ 知， $N_G(X)$ 的每个 p'-元中心化 $\Omega_i(X)$. 由第 VII 章，定理 3.4, $N_G(X)$ 的每个 p'-元

中心化 X. 还有, 由 X 的定义, $N_G(X)/X$ 是 p-幂零的. 这样一来, $N_G(X)$ 为 p-幂零, 矛盾于 X 的定义. 完成 (5) 的证明.

(6) 若 $p=2$, 存在一个 $X\in\chi$ 使得 $\Omega_2(S)\le X$.

假设不真. 首先证明

6-1) 若 $M\le G$, M 非 2-幂零, 而 $\Omega_2(S)\le M$, 则 $G=M$.

令 S_0 是 M 的一个 Sylow 2-子群使得 S_0 包含 $\Omega_2(S)$. 我们有 $\Omega_2(S_0)=\Omega_2(S), N_M(S_0)\le N_G(\Omega_2(S))$. 若 $N_G(\Omega_2(S))$ 不是 2-幂零, 则可以找到一个 $X\in\chi$ 使得 $\Omega_2(S)\le X$, 矛盾于假设. 于是 $N_G(\Omega_2(S))$ 必定 2-幂零, 从而 M 满足定理的假设, 由 G 的极小性得 $M=G$, 6-1) 成立.

接下来证明

6-2) $\Omega_1(S)\le Z(G)$

由 (3) 和 (5) 推出 $\Omega_1(S)\lhd G$, 于是由命题 6.5 得 $\Omega_2(S)\le C_G(\Omega_1(S))\lhd G$. 如果 $C_G(\Omega_1(S))$ 为 2-幂零, 由于 $O_{p'}(G)$=1, 我们知 $C_G(\Omega_1(S))$ 是一个 2-群, 所以能够找到一个 $X\in\chi$ 使得 $\Omega_2(S)\le X$, 矛盾于假设. 现在应用 6-1) 立得 $C_G(\Omega_1(S))=G$, 6-2) 成立.

因为 G 不是 2-幂零的, G 包含一个子群 K 具有下述性质: K 不是 2-幂零的, 而 K 的真子群均为 2-幂零. 由第 VIII 章, 定理 3.4, K 有一个正规 Sylow 2-子群 $T>1$, T 的方次数 ≤ 4. 所以我们可以假设 $T\le\Omega_2(S)$. 记

$$U=T\Omega_1(S)\le\Omega_2(S).$$

由于 $\Omega_1(S)\le Z(G)$, 我们知 $N_G(U)$ 包含 K, 所以 $N_G(U)$ 不是 2-幂零的. 由 (4) 又知, $T\Omega_1(S)\lhd\Omega_2(S)$, 故 $N_G(U)$ 也包含 $\Omega_2(S)$. 由 6-1) 得 $N_G(U)=G$. 置

$$\overline{G}=G/\Omega_1(S),\overline{U}=U/\Omega_1(S).$$

则 $\overline{U}$ 是初等交换 2-群. 于是由 (4) 知, $\overline{G}$-不变子群 $C_{\overline{G}}(\overline{U})$ 包含 $\Omega_2(S)/\Omega_1(S)$. 因为 $\Omega_1(S)\le Z(G)$, 故由 $O_{p'}(G)$=1 可推出 $O_{p'}(\overline{G})=1$. 因此, 若 $C_{\overline{G}}(\overline{U})$ 是 2-幂零的, 则它必为 2-群, 从

而推出 (6) 成立，矛盾. 于是 $C_{\overline{G}}(\overline{U})$ 不是 2-幂零的，再一次应用 6-1) 得 $\overline{G}=C_{\overline{G}}(\overline{U})$. 这样一来， $\overline{K}$ 为幂零，得出 K 为幂零. 这是一个矛盾，于是 (6) 成立.

(7) 反例 G 不存在.

由 (3), (5) 和 (6), 存在 $X\in\chi$ 使得 $\Omega_i(S)\leq X$ 并且 $N_G(X)=G$. 所以 $X\leq O_p(G)$. 如果 $X<O_p(G)$, 由 X 的定义， $G=N_G(O_p(G))$ 为 p-幂零，矛盾于 G 为反例. 于是 $X=O_p(G)\in\chi$. 再一次应用 X 的定义知， $G/O_{pp'}(G)$ 是 p-群. 令 $K/O_{pp'}(G)$ 是一个主因子. 因为 $O_{p'}(G)$=1, K 不可能是 p-幂零，故知 K 满足定理的假设，所以 $K=G$, 从而 $G/O_{pp'}(G)$ 为 p 阶群. 于是 G 含有子群 $L=Q\rtimes\langle w\rangle$, 这里 $\langle w\rangle$ 是循环 p-群， $w^p\in Z(L)$, 而 Q 是 p'-群. 还有， $G=O_p(G)L$.

首先设 $p=2$. 由 G 的极小性得

$$G=\Omega_2(S)L.$$

因为 $w\notin\Omega_2(S)$, 有 $w^4\neq 1$. 设 $o(w)=2^n(n>2)$. 令 $c=w^{2^{n-2}}\in\Omega_2(S)$. 那么 $c\in Z(L)$. 又因 S 的每个 2 阶元在 $N_G(S)$ 中拟中心，由命题 6.5, c^2 中心化 $\Omega_2(S)$, 得出 $c^2\in Z(G)$. 另一方面，由命题 6.6, $w\langle c^2\rangle$ 中心化 $\Omega_1(S)/\langle c^2\rangle$. 由此推出 Q 中心化 $\Omega_1(S)/\langle c^2\rangle$. 考虑 $G/\Omega_1(S)$. 类似的方法可证 Q 中心化 $\Omega_2(S)/\Omega_1(S)\langle c\rangle$. 于是 Q 稳定子群链

$$1\leq\langle c^2\rangle\leq\Omega_1(S)\leq\langle\Omega_1(S),c\rangle\leq\Omega_2(S).$$

由第 VII 章，定理 3.6 得 $[\Omega_2(S),Q]=1$. 从而 G 为 2-幂零，矛盾.

类似地，当 $p>2$ 时，同样导出 G 为 p-幂零，完成证明. □

作为定理 6.8. 的一个应用，我们证明

定理 6.8 *设 N 是群 G 的正规子群. 对 $|N|$ 的每个素因子 p, 令 $P\in\mathrm{Syl}_p(N)$. 假设*

(1) $\Omega_1(P)$ 由 $N_G(P)$ 的 p 阶正规子群生成.

(2) 当 $p=2$ 时， $\Omega_2(P)$ 由 $N_G(P)$ 的 2 阶和 4 阶循环正规子群生成.

那么包含在 N 中的 G-主因子都是循环的.

证　由定理 6.7 并应用归纳知，N 有 Sylow 塔. 令 p 是 $|N|$ 的最大素因子，那么 N 有正规 Sylow p-子群 P, 当然 $P \lhd G$. 显然 G/P 满足定理假设，于是只需证明定理对 G/P 成立.

若 $p=2$, 由第 VII 章，定理 4.3, G 的每个 p'-元平凡作用于 P, 定理当然成立. 故 $p>2$.

令 M 是由 G' 及一切形如 x^{p-1} 的元素生成的子群. 那么 M 中心化 G 的每个正规 p 阶子群. 于是 M 中心化 $\Omega_1(P)$. 由第 VII 章，定理 4.3, M 的每个 p'-元平凡地作用于 P. G 的每个元在 P 上诱导 P 的一个自同构，所有这样的自同构作成一个群 A, 其中由 M 的元诱导的自同构群 B 是 A 的一个子群. 因为 $M \lhd G$, 所以 $B \lhd A$. 又因为 $M/C_M(P)$ 是一个 p-群，故 B 还是一个 p-群. 由 M 的定义知，A/B 是交换群且方次数整除 $p-1$.

现在令 K/L 是一个 G-主因子，$K \leq P$. 那么 A 不可约地作用在 K/L 上，而 B 平凡作用于 K/L. 因为 A/B 是交换群且方次数整除 $p-1$, 由 A 在 K/L 上诱导的自同构作成一个循环群，其方次数整除 $p-1$. 从而 K/L 为 p 阶循环群. 定理证毕.　□

极小子群均正规的有限群叫做 PN-群. 这是一类重要的可解群. Gaschütz 和 Itô 证明 PN-群是可解的并且它的 Fitting 高不超过 3. 所有极大子群都是 PN-群的非 PN-群 (即内 PN-群) 的分类由 Sastry 给出. 班桂宁证明：所有偶阶极大子群都是 PN-群的非 PN-群或是内 PN-群或是 2 阶群与内 PN-群的直积. 所有偶阶二次极大子群都是 PN-群的非 PN-群只有几个群不可解，详细结果可参看班桂宁和李世荣的文章《偶阶二次极大子群都是 PN-群的有限群》，J. of Math. (PRC), 16:4(1996).

习　题

1. (Gaschütz 和 Itô) 证明 PN-群可解且其导群为 2-闭.

2. (M. Asaad) 若 G 的极小子群及 4 阶循环子群均在 G 中类正规 (见上册附录 p.211), 则 G 为超可解.

3. 举一个例子说明 G 的每个 2 阶元属于 $Z(G)$ 但不必 2-幂零.

4. 设 G 为可解群且 $\Phi(G)=1$. 假设 Fitting 子群 $F(G)$ 的每个极小子群正规于 G. 证明 G 是超可解的.

5. 设 S 为 G 的 Sylow 2-子群. 若 S 是交换的并且 S 的每个 2 阶子群在 $N_G(S)$ 中正规, 则 G 为 2-幂零.

§7. 置换条件

定义 7.1 令 G 是一个群, $H \leq G$. 子群

$$P_G(H)=\langle x|x\in G,\langle x\rangle H=H\langle x\rangle\rangle$$

叫做 H 在 G 中的 **置换化子**.

定义 7.2 我们说群 G 满足 **置换条件** 是指, 对每个 $H<G$ 恒有 $H<P_G(H)$. 这时称 G 是一个 PC-群.

这一节我们主要介绍 J.C.Beidleman 和 D.J.S.Robinson 的工作, 他们完整地给出了 PC-群的构造刻划. 张继平的早期工作也起了一定的作用. 但是, 要全部写出有关证明, 篇幅太长, 因此这里只介绍其中最主要的部份. 有兴趣的读者可参阅 On finite groups satisfying the permutizer condition, *J. Algebra*, **191**(1997), 686–703.

首先证明一个引理, 其中 $p=2$ 那部分属于张继平.

引理 7.3 *令 P 是一个 p-群, p 为素数, N 是 P 的一个非平凡的初等交换正规子群, 且在 P 中有一个补子群 X. 如果 $P=\langle y\rangle X$ 对于某个 $y\in P$, 那么当 $p>2$ 时, $|N|=p$; 当 $p=2$ 时, $|N|\leq 4$.*

证 令 P 为极小阶反例. 分两种情形讨论.

(1) $p>2$. 令 $t\in N\cap Z(P), t\neq 1$. 那么 $P/\langle t\rangle$ 满足引理 7.3 的条件, 由 P 的极小性, 结论对 $P/\langle t\rangle$ 成立. 所以 $|N|=p^2, N=\langle u,t\rangle$ 对于某个 $u\in P$. 由假设, $P=N\rtimes X$, 所以 $y=xu^at^b$, 而 $x\in X$. 由于 $[N,P]\leq\langle t\rangle$, 我们有

$$y^p=(xu^a)^pt^{bp}=x^pu^{ap}[u^a,x]^{\binom{p}{2}}=x^p.$$

故得 $y^p \in X$ 且 $|N| = |P : X| = |\langle y\rangle : \langle y\rangle \cap X| = p$, 这是一个矛盾. 因此, 极小反例对 $p > 2$ 不存在.

(2) $p = 2$. 仍令 $t \in N \cap Z(P)$. 结论对 $P/\langle t\rangle$ 成立, 所以 $|N : \langle t\rangle|$ 整除 4, 而 $|N| = 8$. 令 $s\langle t\rangle$ 是 $N/\langle t\rangle \cap Z(P/\langle t\rangle)$ 的一个非单位元. 那么 $N = \langle s, t, u\rangle$ 对某个 $u \in P$, 且 $\langle s, t\rangle \lhd P$. 还有 $[N, P] \le \langle s, t\rangle, [s, P] \le \langle t\rangle$.

因为 $P = N \rtimes X$, 故 $y = xu^a t^b s^c$ 对于适当 $x \in X$ 及整数 a, b, c. 又因 $s^{xu^a t^b s^c} = s^x = s$ 或 st, 经简单计算得

$$y^4 = (xu^a t^b s^c)^4 = (xu^a)^4,$$

且 $[x^2, \langle s, t\rangle] = 1$. 还有 $(xu^a)^2 = x^2(u^a)^{1+x} \in x^2\langle s, t\rangle$, 因此 $y^4 = (xu^a)^4 = x^4$. 最终得 $|N| = |P : X| = |\langle y\rangle : \langle y\rangle \cap X| \le 4$, 矛盾. 引理证毕. □

定理 7.4 (张继平) 令 G 是一个可解 *PC*-群. 则

(1) G 是超可解的当且仅当 G 不含截断 S_4.

(2) 对任意奇数 p, G 是 p-超可解的.

(3) G' 的 Sylow 2-子群 Q 正规于 G, 且 G/Q 超可解.

证 (1) 的必要性是显然的. 现证充分性. 设 G 非超可解, 并设 G 为极小阶反例. 令 N 为 G 的极小正规子群, 则 G/N 超可解, 从而推出 N 为 G 的唯一极小正规子群, 并且 $\Phi(G) = 1$. 于是 $N = F(G)$, 从而 $C_G(N) = N$ (上册第 V 章定理 4.3), 并且 G 有极大子群 M 使得 $G = MN, M \cap N = 1$. 因为 G 是 PC-群, G 有元素 y 使得 $G = \langle y\rangle M = MN$. 又因 G 为可解, 且 $\mathrm{Core}_G(M) = 1$, 所以 $\langle y\rangle \cap M = 1$, 而 $|G : M| = |\langle y\rangle|$ 是某个素数 p 的方幂. 我们可以找到 M 的一个 Sylow p-子群 S 使得 $P = \langle y\rangle S = NS$ 为 G 的一个 Sylow p-子群. 由引理 7.3 知 $|N| = 4$. 考虑 G 关于 M 的陪集 (4 个) 上的置换表示, 立得 $G \cong S_4$. 矛盾于假设.

(2) 类似于 (1) 的证明.

(3) 对任意奇素数 p, 由 (2) 知 G 为 p-超可解. 根据定理 1.8, G' 为 p-幂零. 由此推出 G' 的 Sylow 2-群 Q 是 G 的正规子群. 现

在 G/Q 也是 PC-群，且不含截断 S_4，由 (1) 知 G/Q 为超可解. □

Beidlemant 和 Robinson 指出，定理 7.4 中的可解性条件可以去掉. 更一般地，他们证明了下述定理

定理 7.5 *每个 PC-群是可解的.*

这个定理对于研究 PC-群当然是十分重要的，不过它的证明依赖有限单群分类，因此这里只能割爱，将其证明略去.

定理 7.6 *令 G 是一个 PC-群，那么 G 的每个主因子的阶为素数或 4.*

证 令 G 为极小阶反例，并且令 A 为 G 的一个极小正规子群. 由定理 7.5, G 是可解的，所以 A 是初等交换 p-群. G/A 也是 PC-群，故由 G 的极小性，定理对 G/A 成立，所以 $|A|>p$, 且当 $p=2$ 时，$|A|>4$. 进一步还可推出 A 是 G 的唯一极小正规子群. 令 $N=F(G)$. 由 A 的唯一性知 N 为 p-群，且 $A\le Z(N)$. 记 $F/N=O_{p'}(G/N)$. 那么 $F=N\rtimes V, V\cap N=1$, V 为 p'-群. 由 Frattini 论断，$G=N_G(V)F=LN$, 而 $L=N_G(V)$. 因为 $L\cap A\lhd L$ 且 $A\le Z(N)$, 故有 $L\cap A\lhd LN=G$. 由 A 的极小性得 $L\cap A=1$ 或 $A\le L$.

首先令 $A\le L$. 在这个情形，$[A,V]=1$. 又因 $F=VN$, 故 $A\le Z(F)$. 令 $O_{p'}(G/A)=T/A$. 则 $TN/N\le O_{p'}(G/N)=F/N$, 所以 $T\le F$ 且 $[A,T]=1$. 因此，$T=A\times O_{p'}(T)$. 因为 $O_{p'}(T)\lhd G$, 而 A 为 G 的唯一极小正规子群，推出 $T=A$. 于是 $O_{p'p}(G/A)=O_p(G/A)=N/A$. 由定理 1.4, N/A 是 G/A 的 p-主因子中心化子之交. 这样，当 $p>2$ 时，G/N 是一些阶为 $p-1$ 的循环群直积的子群，而当 $p=2$ 时，G/N 是 S_3 直积的一个子群. 因此，如果 $p>2$, 则 $F=G$, 故 $A\le Z(G)$, 矛盾于 $|A|>p$. 于是 $p=2$, 而 G/N 是 3-群借助一个 2-群的扩张. 因为 $F/N=O_{2'}(G/N)$, 故 G/F 是一个 2-群，但是 G/F 不可约地作用在 A 上，再一次推出 $A\le Z(G)$, 矛盾.

其次令 $A\cap L=1$. 取 G 的子群 U 使得 $L\leq U$ 且 $U\cap A=1$, 并且有尽可能大的阶. 因为 G 是 PC-群, 所以存在 $g\in G\backslash U$ 使得 $\langle g\rangle U=U\langle g\rangle$. 令 $\langle g\rangle=\langle t\rangle\times\langle z\rangle$, t 是 p-元而 z 是 p'-元. 现在 $|\langle g\rangle U:U|$ 整除 $|G:U|=|UN:U|=|N:U\cap N|=p$ 的一个幂. 因此 $\langle g\rangle/U\cap\langle g\rangle$ 是一个 p'-群, 这说明 $z\in U\cap\langle g\rangle$. 因此 $\langle g\rangle U=\langle t\rangle U$, 且 $U\langle g\rangle=\langle t\rangle$. 这意味着我们可以假设 g 是一个 p-元.

现在令 $U^\star=\langle g\rangle U$. 那么 $U^\star\cap A\neq 1$. 但是 $U^\star\cap A\lhd U^\star N=G$, 故由 A 的极小性得 $A\leq U^\star$ 且 $UA\leq U^\star$. 于是

$$UA=(UA)\cap U^\star=(UA)\cap\langle g\rangle U.$$

令 Q 为 UA 的一个 Sylow p-子群且 Q 包含 $UA\cap\langle g\rangle$. 我们有

$$Q=Q\cap(UA)=(Q\cap U)A$$

及

$$Q=Q\cap(UA)=Q\cap((UA\cap\langle g\rangle)U)=(UA\cap\langle g\rangle)(Q\cap U).$$

对 Q 应用引理 7.3 知, 当 $p>2$ 时, $|A|=p$; 当 $p=2$ 时, $|A|=4$. 这是最后的矛盾, 定理证毕. □

推论 7.7 *令 G 是一个 PC-群. 那么 G 的每个极大子群的指数是素数或者 4.*

作为定理 7.6 的一个系, 下述结果是很有新意的.

定理 7.8 *群 G 是超可解的当且仅当 G 与 G' 是 PC-群.*

证　必要性是显然的. 证充分性. 令 G 是一个极小阶反例. 那么 G 有唯一个极小正规子群 N 且 G/N 为超可解. 于是由推论 1.13, $\Phi(G)=1$, 并且应用定理 7.6 得 $|N|=4$. 现在 N 在 G 中有一个补子群 X, 即 $G=NX, N\cap X=1$. 但是 $C_X(N)=N$, 所以 $G=S_4$ 或 A_4, $G'=A_4$ 或 $|G'|=4$. 矛盾于 G 与 G' 都是 PC-群的假设. □

习　题

1. 证明 S_4 是 PC-群.

2. 证明超可解群必是 PC-群.

3. 设 G 是一个 PC-群. 证明 $G/O_{2'}(G)$ 是一个 $\{2,3\}$-群.

4. 设 $H \trianglelefteq G$. H 叫做 G 的超可解嵌入子群, 如果包含在 H 中的每个 G-主因子是循环的. 证明超可解群嵌入子群之积仍为超可解群嵌入子群.

5. 用 $SE(G)$ 表示 G 的所有超可解嵌入子群之积. 证明 G 是 PC-群当且仅当 $G/SE(G)$ 是 PC-群.

§8. 共轭类长

元素的 **共轭类长** 与复数域上不可约特征标的级有许多平行的性质, 因此受到人们的重视, 成为近十年来有限群研究的一个热点. 这里只介绍几个基础性的结果.

令 G 是一个群, $x \in G$ 的共轭类长 $|x^G| = |G : C_G(x)|$. 用 $Con(G)$ 表示 G 的共轭类全体. 一个熟知的结果是 $|\mathrm{Con}(G)| = G$ 的不可约复特征标的个数.

引理 8.1 令 $N \lhd G, x \in N, y \in G$. 则

(1) $|x^N| \mid |x^G|$.

(2) $|(yN)^G| \mid |y^G|$.

证

$$
\begin{aligned}
|x^N| &= |N : C_N(x)| = |N : N \cap C_G(x)| \\
&= |NC_G(x) : C_G(x)| \mid |G : C_G(x)| \\
&= |x^G|.
\end{aligned}
$$

因为 $C_G(y)N/N \leq C_{G/N}(yN)$, 所以

$$
\begin{aligned}
|(yN)^G| &= |G/N : C_{G/N}(yN)| \mid |G/N : C_G(x)N/N| \\
&= |G : C_G(y)N| \mid |G : C_G(y)| = |y^G|.
\end{aligned}
$$

□

定理 8.2 (Chilag-Herzog) 如果对任意 $x \in G, 4 \nmid |x^G|$, 则 G 为可解.

这个定理的原始证明依赖有限单群分类定理，李世荣给出一个初等的并且十分简短的证明. 为此需要

引理 8.3 (Thompson) 令 S 是群 G 的 Syow 2-子群, 且 M 是 S 的一个子群, $|S:M|=2$. 令 u 是 S 的一个对合. 那么或者 u 与 M 的一个元素共轭, 或者 $u \notin G'$.

证　令 $\Omega = \{Mg \mid g \in G\}$. 则 G 作成 Ω 上的置换表示, $|\Omega| = 2|G:S|$. 若 $Mgu = Mg$, 那么 $gug^{-1} \in M$, 结论已成立. 于是可设 u 在 Ω 上无不动点. 因为 $|G:S|$ 是奇数, 故 u 为 Ω 上一个奇置换, 从而知存在 $N \lhd G$ 使得 $|G:N|=2$, 且 $u \notin N$. 结论成立. □

定理 8.2 的证明　由引理 8.1 知, 定理的假设对正规子群及商群保持, 所以我们只需证明 G 是非单的.

假设 G 是一个非交换单群. 由 Feit-Thompson 关于奇数阶群可解定理, G 至少有一个对合 u. 令 S 是 G 的一个 Sylow 2-子群使得 $u \in S$. 置

$$H = C_G(u).$$

由假设

$$|G:C_G(x)|_2 \leq 2,\ \text{对任意}\ x \in G.$$

固定 x, 令 T 为 $C_G(x)$ 的 Sylow 2-子群. 由 Sylow 定理, 存在 $g \in G$ 使得 $T^g \leq S$ 且 $T^g \leq C_G(x^g)$. 若 $u \in T^g$, 则 $u \in C_G(x^g)$, 从而 $x \in C_G(u)^{g^{-1}} = H^{g^{-1}}$. 若 $u \notin T^g$, 则 $|S:T^g|=2$. 因为 G 是单的, 由引理 8.3 得 u 与 T^g 的一个元共轭, 即存在 $h \in G$ 使得 $u^h \in T^g$, 于是 $u^h \in C_G(x^g)$, 得出 $x \in C_G(u^{hg^{-1}}) = H^{hg^{-1}}$. 总之不论哪种情形都有 $x \in \bigcup_{y \in G} H^y$. 由 x 的任意性, G 是 H 的所有共轭的并, 由此得 $G = H$(见上册第 I 章例 7.1), 与 G 的单性矛盾. 定理证毕.

定理 8.4 (Chilag-Herzog) 若群 G 的所有共轭类长无平方因子, 则 G 超可解.

证 令 G 是一个极小阶反例. 由定理 8.2 知 G 为可解. 所以 G 有 p^n 阶极小正规子群 N. 若 $n=1$, 因为 G/N 超可解 (引理 8.1), 得出 G 超可解, 矛盾于假设. 故 $n>1$, 并且 G 没有素数阶正规子群. 若 $N\subseteq\Phi(G)$, 根据推论 1.13, G 为超可解, 再一次矛盾. 因此, G 有极大子群 M 使得 $G=MN, M\cap N=1$, 而 $M\cong G/N$ 为超可解. 令 Q 为 M 的极小正规子群, 则 Q 有素数阶. 置 $Q=\langle x\rangle$. 若 $C_G(x)\cap N\neq 1$, 则 $M<N_G(Q)=G, Q$ 为 G 的素数阶正规子群, 一个矛盾. 因此

$$p^n \mid |NC_G(x):C_G(x)| \mid |G:C_G(x)|.$$

而 $n>1$, 矛盾于假设. 定理证毕. □

引理 8.5 (Wielandt) 令 G 是一个群, p 为一个素数, $x\in G$. 如果 $o(x), |x^G|$ 均为 p 的方幂, 则 $x\in O_p(G)$.

证 令 P 是 G 的一个 Sylow p-子群使得 $x\in P$, 则 $G=C_G(x)P$. 因此 $\langle x\rangle^G=\langle x\rangle^{C_G(x)P}=\langle x\rangle^P\leq P$, 从而 $\langle x\rangle^G\subseteq O_p(G)$. 引理成立. □

定理 8.6 令 p 是一个固定奇素数. 假设对于 G 的任一 p 阶元 x, $|x^G|$ 是素数幂, 则 G 为 p-可解.

证 令 G 是一个极小阶反例.

(1) G 的每个真正规子群为 p-可解, 且 $O_{p'}(G)=1$.

这由引理 8.1 及 G 的极小性推出.

(2) $O_p(G)>1$

由上册第 VI 章定理 5.2, G 不是非交换单群. 令 N 为 G 的极小正规子群, 则 $1<N<G$, 并且由 (1) 知 N 是 p-可解的. 因为 $O_{p'}(N)\leq O_{p'}(G)$=1, 故 $O_{p'}(N)=1$, 从而 $O_p(G)\geq O_p(N)>1$.

(3) G 的所有 p 阶元含于 $O_p(G)$ 中.

设存在一个 p 阶元 $x \in G$ 使得 $x \notin O_p(G)$. 由假设 $|G : C_G(x)| = r^n$, 而 r 是一个素数. 由引理 8.5 知 $r \neq p$. 因此 $C_G(x)$ 包含 G 的一个 Sylow p-子群, 当然 $O_p(G) \subseteq C_G(x)$. 记 $C = C_G(O_p(G))$, 则 $x \in C \lhd G$, 且 $O_p(C) \leq O_p(G)$. 因 $x \notin O_p(G)$, 得 $O_p(C) < C$. 如果 $C < G$, 则 C 为 p-可解, 于是 $O_{pp'}(C) > O_p(C)$. 由于 C 的每个元中心化 $O_p(C)$, 我们有

$$O_{pp'}(C) = O_p(C) \times H,$$

这里 $H > 1$ 是 p'-群. 因为 $O_{pp'}(C)$ 是 C 的特征子群, 且 $C \lhd G$, 得出 $1 < H \leq O_{p'}(G)$, 矛盾于 (1). 因此我们能够断言 $C = G$, 即 $O_p(G) \leq Z(G)$.

考察商群 $\overline{G} = G/O_p(G)$. 显然 $\overline{x} = O_p(G)x$ 是 $\overline{G}$ 的一个 p 阶元, 而且

$$|\overline{G} : C_{\overline{G}}(\overline{x})| \mid |G : C_G(x)| = r^n.$$

再一次应用上册第 VI 章定理 5.2 知, G 有正规子群 N 使得 $O_p(G) < N < G$, 并且由 (1) 知 N 为 p-可解. 于是 $O_p(N) \leq O_p(G) \leq Z(G)$, 且

$$O_{pp'}(N) > O_p(N).$$

从而得出 $O_{p'}(G) > 1$, 与 (1) 矛盾. (3) 被证明.

(4) G/M 是非交换单群, 且 $p \mid |G : M|$, 这里 M 是 G 的最大 p-可解正规子群.

这由 (1) 推出.

(5) G 不存在.

令 S_0 是 M 的一个 Sylow 2-子群, 并置

$$H = N_G(S_0).$$

由 Frattini 论断 $G = MH$. 由 (4) 知 $H/H \cap M \cong G/M$ 是非交换单群, 且 $p \mid |H/H \cap M|$. 由 (3) 推出 H 的每个 p 阶元含于 $H \cap O_p(G) \leq O_p(H)$. 令

$$C = C_H(O_p(H)).$$

由定理 6.1 知 C 为 p-幂零. 因此 $(H\cap M)C/H\cap M \cong C/H\cap M$ 也是 p-幂零. 然而 $(H\cap M)C/H\cap M$ 是非交换单群 $H/H\cap M$ 的正规子群, 这就迫使 $C \le H\cap M$.

由 Feit-Thompson 关于奇数阶群可解定理, G 有 Sylow 2-子群 S 使得 $S_0 < S$ 并且 $S \le H$. 选取 S_1/S_0 为 $Z(S/S_0)$ 的一个 2 阶子群. 我们有 $S_1 = S_0\langle u\rangle$, 而 $u^2 \in S_0, S_1 \lhd S$.

考察子群 $K = O_p(H) \rtimes S_1$. 若 $S_1 \lhd K$, 则 $S_1 \le C_H(O_p(H)) = C \le H\cap M$, 矛盾于 S_0 是 M 的 Sylow 2-子群. 因此 K 无正规 Sylow 2-子群, 当然 K 不是幂零群. 令 W 为 K 的非幂零子群中极小者. 那么 W 是极小非幂零群, 且 $|W|$ 仅有因子 2 和 p, W 还有正规 Sylow p-子群. 由第 VIII 章定理 3.4

$$W = X \rtimes \langle v\rangle.$$

这里 $o(v)$ 为 2 的幂, $\Phi(\langle v\rangle) = \langle v^2\rangle \le Z(W)$, 而 X 是方次数为 p 的 p-群. $\langle v\rangle$ 不可约地作用在 $X/\Phi(X)$ 上, v 诱导 $X/\Phi(X)$ 的一个 2 阶自同构, 推出 $X/\Phi(X)$ 为 p 阶群, 从而 $X = \langle x\rangle$ 的阶为 p. 还有 $S_0 \le C_G(x) < N_G(\langle x\rangle)$, 所以 $N_G(\langle x\rangle)$ 包含 K 的 Sylow 2-子群 $S_0\langle v\rangle$. 不失一般性, 可设 $S_1 = S_0\langle v\rangle$. 现在, 由于 $|N_G(\langle x\rangle)/C_G(x)|_2 > 1$ 并引用定理的假设, 我们得到

$$|G : C_G(x)| = 2^n, n \ge 1.$$

因此

$$G = N_G(\langle x\rangle)S.$$

若 $G = N_G(\langle x\rangle)$, 则 $C_G(x) \lhd G$. 由 (1), $C_G(x)$ 为 p-可解, 从而 G 为 p-可解. 故可设 $N_G(\langle x\rangle) < G$. 由于 $S_1 < S$, 我们得到

$${S_1}^G = {S_1}^{SN_G(\langle x\rangle)} = {S_1}^{N_G(\langle x\rangle)} \le N_G(\langle x\rangle).$$

因为 ${S_1}^G$ 为 p-可解, 而 M 为 G 的最大 p-可解正规子群, 所以 ${S_1}^G \le M$. 这样一来

$$|M|_2 = |S_0| < |S_1| \le |M|_2.$$

这是最后一个矛盾, 完成证明.

推论 8.7 若群 G 的每个素数阶元的共轭类长是素数幂, 则 G 为可解.

令 p 是一个素数, G 的元 x 叫 p-正则的, 如果 x 的阶与 p 互素. p-正则元的共轭类简称 p-正则共轭类. p-正则共轭类与模表示有密切关系.

定理 8.8 (任永才) 令 p 为任一素数. 假设对每个 p-正则元 x, 恒有 $p \nmid |x^G|$, 则 $G = O_p(G) \times O_{p'}(G)$.

证 令 $P \in \mathrm{Syl}_p(G)$ 且 $K = PC_G(P)$. 令 $x \in G$. 写 $x = x_p x_{p'}$, 而 $x_p, x_{p'}$ 分别为 x 的 p-部分和 p' 部分. 由假设, G 有元 g 能使 $P^g \subseteq C_G(x_{p'})$. 另一方面, $x_p \in C_G(x_{p'})$, 所以存在 $z \in C_G(x_{p'})$ 使得 ${x_p}^z \in P^g$. 从而得 $x^z = {x_p}^z {x_{p'}}^z = {x_p}^z x_{p'} \in P^g C_G(P^g) = K^g$. 于是由 x 的任意性得 $G = \bigcup_{g\in G} K^g$. 因此 $G = K$, 结论成立. □

定理 8.9 (任永才) 令 G 为可解群, p 为素数. 假设对于每个 p-正则元 x, $p^2 \nmid |x^G|$, 则 G 的 p-长 $l_p(G) \le 2$.

在证明定理 8.9 之前, 我们先证明下面的引理.

引理 8.10 设 $G = V \rtimes P$ 满足定理 8.9 的条件. p-群 P 忠实地作用在 p'-初等交换群 V 上, 则 $|P| = p$.

证 对 P 的阶用归纳法. 显然 P 的极大子群 P_1 也忠实地作用于 V, 而且 $P_1V \lhd G$. 由引理 8.1, 结论对 P_1V 成立. 故 $|P| = p^2$. 还有, 因为 V 是交换的, 容易证明对每个 $1 \ne x \in V$ 恒有 $C_P(x) > 1$.

我们来证明, 不可能存在 P-不变的子群 V_1 和 V_2 满足下列三个条件:

1) $V_1 \cap V_2 = 1$.

2) 存在 $x \in V_1, y \in V_2$, 使得 $A = C_P(x)$ 与 $B = C_P(y)$ 同为 p 阶群.

3) $P = A \times B$. 因为若有这样的 V_1, V_2, 那么由

$$(xy)^{ab} = x^b y^a = xy \quad \forall a \in A \text{ 和 } b \in B.$$

能推出 $x^{-1}x^b = yy^{a^{-1}} \in V_1 \cap V_2 = 1$, 从而 $x^b = x, y^a = y$, 得出 $a = b = 1$. 这样一来, $C_P(xy) = 1$, 矛盾.

现在因 P 忠实作用于 V, 故可置

$$C = C_V(P) < V.$$

取 $x \in V \backslash C$, 则 $A = C_P(x)$ 为 p 阶群. 令 $V_1 = C_V(A)$. 则 V_1 为 P-不变, 且 $V_1 < V$. 根据 Maschke 定理 (上册第 VI 章引理 3.15), V_1 有 P-不变补子群 V_2. 若 $V_2 \leq C$, 则 A 平凡作用于 $V_1 \times V_2 = V$, 与忠实的条件矛盾. 因此 $V_2 \not\leq C$. 故存在 $y \in V_2 \backslash C$, 使得 $B = C_P(y)$ 为 p 阶群. 易知 $A \neq B$, 所以 $P = A \times B$, 并且 V_1 和 V_2 满足条件 1)–3), 这是一个矛盾. □

定理 8.9 的证明: 由引理 8.1 知 $G/O_p(G)$ 满足定理假设, 故只需证明 $G/O_p(G)$ 的 p-长 ≤ 1. 不失一般性, 可设 $O_p(G) = 1$. 首先证明 G 的 p-秩 $r_p(G) \leq 1$. 用 V 表示 G 的极小正规子群. 因为 $O_p(G) = 1$, 故 V 是 p'-初等交换群. 令 $O_p(G/V) = N/V, Q \in \mathrm{Syl}_p(N)$. 若 $O_p(G/V) = 1$, 由归纳, 结论对 G/V 成立, 从而结论对 G 成立. 因此可设 $Q > 1$.

现在, $N = V \rtimes Q \lhd G$, 而 $Q \neq 1$ 为 p-群, Q 忠实作用于 V. 由引理 8.10 知 $|Q| = p$. 因 $O_p(G/N) = 1$, 应用归纳得 $r_p(G/N) \leq 1$. 于是 G 的每个 p-主因子都是 p 阶群, 即 $r_p(G) \leq 1$.

现在 G 是可解群且 $r_p(G) \leq 1$, 由定理 2.6 得 $l_p(G) \leq 1$, 完成证明.

关于 p-正则共轭类长的进一步结果见

[1] 任永才, On the length of p-regular classes and the p-structure of finite groups, Agebra Colloq., 2:1(1995),3–10.

[2] 任永才, On the length of the p-regular classes of finite groups, 科学通报, 39(1994),301–303.

在结束本章之前, 我们向读者推荐张继平关于共轭类的一个出色的结果, 见张继平的文章, Finite groups with many conjugate elements, J. Algebra **170**(1994), No.2, 608–624.

习 题

1. (Itô) 若群 G 恰好有两个共轭类长 1 和 m, 则 G 为可解.

2. 设 p 为固定素数, 若对一切 $x \in G \backslash Z(G)$, $|C_G(x)|$ 是 p 的幂, 则 G 为交换群或者 p-群.

3. 设对一切 $x \in G \backslash Z(G)$, $|C_G(x)|$ 无立方因子, 则 G 为交换群或 $|G|$ 无立方因子.

4. 设 π 是一个素数集. 假设 G 的每个共轭类长是一个 π-数, 那么 $G = G_1 \times G_2$, 这里 G_1 是一个 π-子群而 G_2 是交换 π'-子群.

第 X 章

有限 p-群的进一步知识

本章继续第 IV 章讲述有限 p-群的进一步知识，将沿用第 IV 章中所采用的符号和术语.

只对有限 p-群感兴趣的读者可在阅读完第 IV 章后直接阅读本章而跳过其它各章.

§1. Hall 恒等式

本节中证明对正则 p-群和 p-群幂结构理论十分重要的 P. Hall 恒等式. 这里讲述的是经过 J. Petrescu 改进了的形式. 即下面的

定理 1.1 (P. Hall 和 J. Petrescu) *设 G 是群, $x, y \in G$, $H = \langle x, y \rangle$. 再设 m 是任一给定的正整数. 则存在 $c_i \in H_i$, (这里 H_i 是 H 的下中心群列的第 i 项), $i = 2, 3, \cdots, m$, 使得*

$$x^m y^m = (xy)^m c_2^{\binom{m}{2}} c_3^{\binom{m}{3}} \cdots c_m^{\binom{m}{m}}. \tag{1.1}$$

证 考虑 $2m$ 秩自由群 F, 它的自由生成系 $X = \{x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_m\}$, 且设 $X \cap G = \varnothing$. 令 $X_i = \{x_i, y_i\}$, $i = 1, 2, \cdots, m$. 再令 $M = \{1, 2, \cdots, m\}$, 即 X 中元素的下标的集合, 于是 $X = \bigcup_{i=1}^m X_i$. 我们对 M 的所有非空子集所组成的集合 $\mathfrak{M}$ 编一个良序: 设 $S, T \in \mathfrak{M}$, 规定 $S < T$, 如果 $|S| < |T|$, 或者 $|S| = |T|$, 但在字典式编序中 S 先于 T. (注意在字典式编序下比较子集 S 和 T, 应先把 S 和 T 中的元素按由小到大的顺序排列, 然后再

比较.）这样，在 $\mathfrak{M}$ 中 m 个单元素集 $\{1\},\{2\},\cdots,\{m\}$ 排在最前面，接着是二元子集 $\{1,2\},\{1,3\},\cdots,\{1,m\},\{2,3\},\cdots,\{2,m\},\cdots,\{m-1,m\}$，再接着是三元子集 $\{1,2,3\},\cdots$，最后是 M 集合本身.

对于任意的 $S\in\mathfrak{M}$，我们令 $X_S=\bigcup_{i\in S}X_i$. 并规定

$$F_S=F_{|S|}\cap\langle X_S\rangle, \tag{1.2}$$

其中 $F_{|S|}$ 是 F 的下中心群列的第 $|S|$ 项. 我们断言 F_S 是 F 的子群，并且任一由 X_S 中元素作成的权 $\geq|S|$ 的换位子均在 F_S 中. (如下归纳地定义换位子的权：首先，X 中的元素 $x_i,y_j,\cdots$ 均看成是权为 1 的换位子，并规定由一个权为 r 的换位子和一个权为 s 的换位子再作换位运算得到的换位子的权为 $r+s$.) 我们以权为 2 的换位子 $[x_2,y_1]$ 为例来说明上述事实：这时有 $S=\{1,2\}$，因为

$$[x_2,y_1]\in\langle x_2,y_1\rangle\leq\langle X_S\rangle,$$

而 $|S|=2$，故

$$[x_2,y_1]\in F_{|S|}\cap\langle X_S\rangle.$$

同理可知这个事实对权 >2 的换位子也成立.

下面设

$$g=x_1x_2\cdots x_my_1y_2\cdots y_m. \tag{1.3}$$

我们将用 P. Hall 所谓的集积过程 (collecting process) 把它变成下面形式：

$$g=\prod_{S\in\mathfrak{M}}f_S, \tag{1.4}$$

其中 f_S 是 F_S 的适当元素，并且乘积中因子的顺序是依其下标在上面规定的 $\mathfrak{M}$ 的良序来排列.

首先，我们给由 X 中元素组成的每个换位子附加一个标记，即所有在其中出现的元素的下标所组成的集合，它是 M 的一个非空子集，于是属于 $\mathfrak{M}$. X 中元素本身是权为 1 的换位子，它的标记即其下标，看成是 M 的单元素子集. 而换位子 $[x_2,y_1],[x_1,y_2]$

和 $[y_1,x_2]$ 等都有下标 $\{1,2\}$, 依此类推. 集积过程的方法也很简单, 只是反复运用公式:

$$\cdots ba\cdots = \cdots ab[b,a]\cdots, \tag{1.5}$$

这里 a 和 b 是两个由 X 中元素组成的换位子, a 的标记先于 b 的标记. 公式 (1.5) 把 a 调到 b 前面, 同时产生一个新换位子 $[b,a]$, 整个乘积的值并不改变. 因为新产生的换位子 $[b,a]$ 的标记必后于 a 的标记, 又不会先于 b 的标记, 这就使得 (1.5) 式右边三个换位子的下标的次序是依 $\mathfrak{M}$ 的良序排列.

现在我们由 (1.3) 式出发, 应用 (1.5) 式逐次把具有最小标记 S 的元素调到最前面, 并记其乘积为 f_S. 由于在使用公式 (1.5) 时产生的新换位子的标记必后于 S, 这样的过程必在有限步终止, 于是可将 (1.3) 式化成 (1.4) 式的形式. 更具体地说, $\mathfrak{M}$ 的最小元为 $\{1\}$. 在 (1.3) 式中具有该标记的因子为 x_1 和 y_1, 我们需把 y_1 调到前面紧挨着 x_1 的位置, 即把 (1.3) 式变成

$$g = x_1y_1x_2[x_2,y_1]x_3[x_3,y_1]\cdots x_m[x_m,y_1]y_2\cdots y_m,$$

命 $f_{\{1\}} = x_1y_1$, 而 $f_{\{1\}}$ 后面的诸因子, 包括原来的 $x_2,\cdots, x_m$, $y_2,\cdots, y_m$ 以及新产生的 $m-1$ 个权为 2 的换位子 $[x_2,y_1], [x_3,y_1]$, $\cdots, [x_m,y_1]$ 的标记均后于 $\{1\}$. 称它们的乘积为未整理部分, 其中诸因子的标记最小者为 $\{2\}$, 有其标记的元素为 x_2 和 y_2, 这又要求我们把 y_2 调到前面紧挨 x_2 的位置, 这样的调动又将产生一些标记后于 $\{2\}$ 的换位子. 命 $f_{\{2\}} = x_2y_2$, 在新的未整理部分中所有因子的标记将均后于 $\{2\}$. 然后再取其最小者 $\{3\}$, 进行同一过程. 由于 $\mathfrak{M}$ 只含有限多个元素, 这样的过程将在有限步终止, 而 (1.3) 式就变成了 (1.4) 式. 为了彻底弄清楚这点, 建议读者以 $m=3$ 为例, 亲自做一下这样的集积过程, 并求出所有的 f_S.

现在定义一个由 F 到 G 的子群 $H=\langle x,y\rangle$ 上的同态映射 ε, 它在 F 的生成系 X 上的作用为

$$x_i^\varepsilon = x,\ y_i^\varepsilon = y,\ i=1,2,\cdots,m.$$

我们断言,在 (1.4) 式的因子中,如果 $S_1, S_2 \in \mathfrak{M}$, 且 $|S_1| = |S_2| = s$, 则 $f_{S_1}^{\varepsilon} = f_{S_2}^{\varepsilon}$. 于是若令其公共值为 c_s, 因 M 的势为 s 的子集个数为 $\binom{m}{s}$, 以 ε 作用到 (1.4) 式上, 即得到所需的 (1.1) 式, 从而完成定理的证明. 下面用对 s 的归纳法来证明这点: 若 $s=1$, 可令 $S_1 = \{i_1\}$, $S_2 = \{i_2\}$, 由集积过程容易看出

$$f_{S_1} = x_{i_1} y_{i_1}, \qquad f_{S_2} = x_{i_2} y_{i_2},$$

于是 $f_{S_1}^{\varepsilon} = f_{S_2}^{\varepsilon} = xy$, 结论成立. 现在设 $s > 1$. 由 (1.3) 和 (1.4) 式得到

$$\prod_{i=1}^{m} x_i \prod_{i=1}^{m} y_i = \prod_{S \in \mathfrak{M}} f_S. \tag{1.6}$$

如果对于任意的 $j \notin S_1$, 令 $x_j = y_j = 1$, 则易见只要 $S \not\subset S_1$, 在 (1.6) 式中的因子 $f_S = 1$, 于是 (1.6) 式变为

$$\prod_{i \in S_1} x_i \prod_{i \in S_1} y_i = \Big(\prod_{\varnothing \neq T \subsetneq S_1} f_T \Big) f_{S_1}.$$

用 ε 去作用则得

$$x^s y^s = \Big(\prod_{\varnothing \neq T \subsetneq S_1} f_T^{\varepsilon} \Big) f_{S_1}^{\varepsilon}. \tag{1.7}$$

用同样的方法对于子集 S_2 可得

$$x^s y^s = \Big(\prod_{\varnothing \neq T \subsetneq S_2} f_T^{\varepsilon} \Big) f_{S_2}^{\varepsilon}. \tag{1.8}$$

依归纳假设, f_T^{ε} 的值只依赖于 $|T|$. 因为对任意的正整数 $t < s$, 在 S_1 和 S_2 中有相同多个势为 t 的子集, 于是有

$$\prod_{\varnothing \neq T \subsetneq S_1} f_T^{\varepsilon} = \prod_{\varnothing \neq T \subsetneq S_2} f_T^{\varepsilon}.$$

由此, 结合 (1.7), (1.8) 二式即可得到 $f_{S_1}^{\varepsilon} = f_{S_2}^{\varepsilon}$. 定理证毕. □

§2. 正则 p-群和 p-交换群

1933 年，P. Hall 发表了著名论文 "A contribution to the theory of groups of prime-power order", (载 *Proc. London Math. Soc.*, **36**(1933), 29–95). 这篇论文是有限 p-群理论的奠基性论文，其中以大约一半的篇幅讲述了他所创建的正则 p-群的理论. (上节讲述的 P. Hall 恒等式的第一个证明就出现在这篇文章中.) 两年之后，他又在题为 "On a theoram of Frobenius" (载 *Proc. London Math. Soc.*, **40**(1935/36), 468–501) 的论文中发展了这个理论. 此后的半个世纪中，又有一些人对这个理论做了不少有价值的工作，使它形成了 p-群理论中的一个重要的研究方向.

我们将从本节起，用三节的篇幅讲述正则 p-群的基本知识.

首先我们规定一下符号. 设 G 是有限 p-群，如前一样，我们以

$$G = G^{(0)} > G^{(1)} = G' > G^{(2)} > \cdots > G^{(r)} = 1,$$

$$G = G_1 > G_2 = G' > G_3 > \cdots > G_{c+1} = 1,$$

和

$$1 = Z_0(G) < Z_1(G) = Z(G) < \cdots < Z_c(G) = G$$

分别表示 G 的*导群列*，*下中心群列*和*上中心群列*, $r = r(G)$ 和 $c = c(G)$ 表示群 G 的*导列长*和*幂零类*. 并以 $d(G)$ 表群 G 的*秩*, 即满足 $p^{d(G)} = |G/\Phi(G)|$ 的正整数 $d(G)$.

设 $\exp G = p^e$, 称 $e = e(G)$ 为群 G 的*幂指数*. 对于任意的 s, $0 \le s \le e$, 我们规定

$$\Lambda_s(G) = \{a \in G \mid a^{p^s} = 1\}, \qquad V_s(G) = \{a^{p^s} \mid a \in G\}.$$

并且规定

$$\Omega_s(G) = \langle \Lambda_s(G) \rangle, \qquad \mho_s(G) = \langle V_s(G) \rangle.$$

于是得到群列

$$1 = \Omega_0(G) \le \Omega_1(G) \le \cdots \le \Omega_e(G) = G$$

和

$$G = \mho_0(G) \geq \mho_1(G) \geq \cdots \geq \mho_e(G) = 1,$$

分别称其为群 G 的*上幂群列*(或 Ω-*群列*) 和*下幂群列*(或 $\mho$-*群列*).

再规定 $\omega(G)$ 为满足 $p^{\omega(G)} = |G/\mho_1(G)|$ 的正整数，于是由 $\Phi(G) = G'\mho_1(G)$ 有 $d(G) \leq \omega(G)$.

在给出正则 p-群的定义之前，我们先引进 p-交换群的概念，并来研究它的一些初步性质.

定义 2.1 称有限 p-群 G 为 *p-交换群*, 如果对任意的 $a, b \in G$, 恒有

$$(ab)^p = a^p b^p.$$

显然，交换群和幂指数为 1 的群都是 p-交换群，但反过来不真. 例如，对于 $p > 2$, p^3 阶的非交换亚循环群为 p-交换群.

下面的定理给出了 p-交换群的初步性质.

定理 2.2 *设 G 是有限 p-交换 p-群，$e(G) = e$. 则对 $0 \leq s \leq e$, 有*

(1) $(ab)^{p^s} = a^{p^s} b^{p^s}$, $\forall a, b \in G$, *即 G 也是 p^s-交换群;*

(2) *映射 $\pi_s : a \mapsto a^{p^s}, a \in G$, 是 G 的自同态;*

(3) $\Lambda_s(G) = \Omega_s(G), V_s(G) = \mho_s(G)$, *且* $G/\Omega_s(G) \cong \mho_s(G)$;

(4) $[a^{p^s}, b] = [a, b^{p^s}] = [a, b]^{p^s}$, *其中 a, b 是 G 的任意元素;*

(5) $\mho_1(G) \leq Z(G)$;

(6) $\mho_1(G') = 1$.

证 (1) 用对 s 的归纳法. 若 $s = 0$, 则结论是显然的. 现设 $s > 0$. 用归纳假设可得

$$(ab)^{p^s} = ((ab)^p)^{p^{s-1}} = (a^p b^p)^{p^{s-1}} = (a^p)^{p^{s-1}} (b^p)^{p^{s-1}} = a^{p^s} b^{p^s},$$

结论成立.

(2) 由 (1) 显然.

(3) 由 π_s 是 G 的自同态，有 $\mathrm{Ker}\ \pi_s = \Lambda_s(G)$ 是 G 的子群，于是 $\Lambda_s(G) = \Omega_s(G)$; 又有 $\mathrm{Im}\ \pi_s = V_s(G)$ 是 G 的子群，于是 $V_s(G) = \mho_s(G)$. 最后由同态基本定理有 $G/\Omega_s(G) \cong \mho_s(G)$.

(4) $[a,b]^{p^s} = (a^{-1}b^{-1}ab)^{p^s} = a^{-p^s}(b^{-1}ab)^{p^s} = a^{-p^s}b^{-1}a^{p^s}b = [a^{p^s},b]$; 同理， $[a,b]^{p^s} = [a,b^{p^s}]$.

(5) 对于任意的 $a,b\in G$, 有

$$b^{-1}a^pb = (b^{-1}ab)^p = b^{-p}a^pb^p,$$

于是 $b^{-(p-1)}a^pb^{p-1} = a^p$, 即 $b^{p-1} \in C_G(a^p)$. 设 $o(b) = p^i$. 因 $(p-1,p^i)=1$, 存在整数 j 使

$$(p-1)j \equiv 1 (\mathrm{mod}\ p^i).$$

于是 $b = (b^{p-1})^j \in C_G(a^p)$. 由 b 的任意性，有 $a^p\in Z(G)$. 再由 a 的任意性即得 $\mho_1(G)\le Z(G)$.

(6) 对任意的 $a,b\in G$, 由 (5) 有 $[a^p,b]=1$. 再由 (4) 得 $[a,b]^p = 1$, 即 $[a,b]\in\Omega_1(G)$. 故 $G'\le\Omega_1(G)$. 又据 (3), 得 $\exp G'\le p$, 于是 $\mho_1(G')=1$. □

下面定义正则 p-群，它是比 p-交换群更宽的一个群类.

定义 2.3 称有限 p-群 G 为 正则的, 如果对任意的 $a,b\in G$, 有

$$(ab)^p = a^pb^pd_1^pd_2^p\cdots d_s^p,$$

其中 $d_i\in\langle a,b\rangle', i=1,2,\cdots,s$, $\langle a,b\rangle'$ 是 $\langle a,b\rangle$ 的导群，而 s 可依赖于 a,b.

显然，正则 p-群的任一子群和商群仍为正则的.

p-交换群也是正则的，但反过来不真. 我们有

定理 2.4 正则 p-群 G 是 p-交换的当且仅当 $\mho_1(G')=1$.

证 由定理 2.2(6) 只须证充分性. 设 G 是正则 p-群，$a,b\in G$. 则由定义 2.3 有

$$(ab)^p = a^pb^pd_1^pd_2^p\cdots d_s^p, d_i\in\langle a,b\rangle',\ \forall i.$$

因 $\mho_1(G')=1$, 有 $\mho_1(\langle a,b\rangle')=1$, 于是 $d_i^p=1$. 由此得 $(ab)^p=a^pb^p$, 即 G 是 p-交换群. □

下面的定理给出正则性的几个充分条件.

定理 2.5 设 G 是有限 p-群.

(1) 若 $c(G)<p$, 则 G 正则;

(2) 若 $|G|\le p^p$, 则 G 正则;

(3) 若 $p>2$ 且 G' 循环, 则 G 正则;

(4) 若 $\exp G=p$, 则 G 正则.

证 (1) 设 $a,b\in G$. 令 $H=\langle a,b\rangle$. 由 Hall 恒等式有

$$a^pb^p=(ab)^pc_2^{\binom{p}{2}}c_3^{\binom{p}{3}}\cdots c_{p-1}^{\binom{p}{p-1}}c_p, \tag{2.1}$$

其中 $c_i\in H_i\le H', i=2,3,\cdots,p-1$, 而 $c_p\in H_p$. 因 $c(G)<p$, 有 $G_p=1$, 自然也有 $H_p=1$, 于是 $c_p=1$. 又由 $p\mid\binom{p}{i}, i=2,\cdots,p-1$, 令 $d_i=c_i^{-\binom{p}{i}/p}$, 则有

$$(ab)^p=a^pb^pd_{p-1}^pd_{p-2}^p\cdots d_2^p,$$

遂得 G 的正则性.

(2) 由 $|G|\le p^p$ 得 $c(G)<p$. 由 (1) 即得结论.

(3) 设 $a,b\in G$, 令 $H=\langle a,b\rangle$. 显然可设 H 非交换, 于是由 G' 循环得 $H'=\langle x\rangle$ 循环, 从而 $H_3\le\langle x^p\rangle$. 由 $p>2$, 有 $H_p\le\langle x^p\rangle$. 应用 Hall 恒等式 (2.1), 对于 $i=2,\cdots,p-1$, 和 (1) 相同, 令 $d_i=c_i^{-\binom{p}{i}/p}$. 而因 $H_p\le\langle x^p\rangle$, 可找到 H' 中元素 d_p 使 $d_p^p=c_p^{-1}$, 于是得到

$$(ab)^p=a^pb^pd_p^pd_{p-1}^p\cdots d_2^p,$$

故 G 正则.

(4) 这是 p-交换群为正则群的特款. □

下面的定理给出正则 p-群幂结构的两个最重要的性质.

定理 2.6 设 G 是有限正则 p-群， s 是任一正整数. 则有

(1) 对任意的 $a,b \in G$, 存在 $c \in G$ 使得 $a^{p^s}b^{p^s} = c^{p^s}$. 于是有 $\mho_s(G) = V_s(G)$;

(2) 对任意的 $a,b \in G$, $a^{p^s} = b^{p^s}$ 当且仅当 $(a^{-1}b)^{p^s} = 1$. 特别地有 $\Omega_s(G) = \Lambda_s(G)$.

证 (1) 先设 $s = 1$, 用对 $|G|$ 的归纳法. 当 $|G| \le p^2$ 时， G 是交换群，结论显然成立. 现在设 $|G| > p^2$. 如果 $\langle a, b\rangle$ 是 G 的真子群，由归纳假设，结论成立. 故可设 $G = \langle a, b\rangle$. 由正则性的定义有

$$a^pb^p = (ab)^p d_1^p \cdots d_s^p, d_i \in G'.$$

因等式右边属于 G 的真子群 $\langle ab, G'\rangle$, 故存在元素 $c \in \langle ab, G'\rangle$ 使

$$(ab)^p d_1^p \cdots d_s^p = c^p,$$

结论成立.

下面设 $s > 1$. 用对 s 的归纳法. 由归纳假设我们有

$$a^{p^s}b^{p^s} = (a^p)^{p^{s-1}}(b^p)^{p^{s-1}} = t^{p^{s-1}},$$

其中 $t \in \langle a^p, b^p\rangle$. 但由结论对 $s = 1$ 已经成立，故存在 $c \in G$ 使 $t = c^p$, 于是 $a^{p^s}b^{p^s} = c^{p^s}$, 结论成立.

(2) 同样先设 $s = 1$, 并用对 $|G|$ 的归纳法. 与前相同可设 $G = \langle a, b\rangle$. 若 $a^p = b^p$, 则 $[a^p, b] = 1$, 即 $a^{-p}(b^{-1}ab)^p = 1$. 因 $\langle a, b^{-1}ab\rangle = \langle a, [a,b]\rangle$ 是 G 的真子群, 由归纳假设即得 $(a^{-1}b^{-1}ab)^p = [a,b]^p = 1$. 因 $G' = \langle [a,b]^g \mid g \in G\rangle$ 也是 G 的真子群，再用归纳假设得 $\exp G' \le p$, 于是由定理 2.4 G 是 p-交换的, 自然可得到 $(a^{-1}b)^p = 1$. 反过来，设 $(a^{-1}b)^p = 1$. 我们有 $G = \langle a^{-1}b, a\rangle$. 与前相同，由 $[(a^{-1}b)^p, a] = 1$ 可推得 $\exp G' \le p$, 于是 G 亦为 p-交换群，故得 $a^{-p}b^p = 1$, 即 $a^p = b^p$.

下面设 $s > 1$. 用对 s 的归纳法. 由归纳假设， $a^{p^s} = b^{p^s}$ 等价于 $(a^{-p}b^p)^{p^{s-1}} = 1$. 考虑 $\overline{G} = G/\Omega_{s-1}(G)$, 设 a, b 在自然同态下的象为 $\bar{a}, \bar{b}$. 则上式即 $\bar{a}^p = \bar{b}^p$(在 $\overline{G}$ 中), 由结论对 $s = 1$ 成立，这

又等价于 $(\bar{a}^{-1}\bar{b})^p = \bar{1}$, 即 $(a^{-1}b)^p \in \Omega_{s-1}(G)$, 或 $(a^{-1}b)^{p^s} = 1$. 结论成立. □

在本节的最后, 我们再证明一个正则性的充分条件, 这也是 P. Hall 最早证明的. 但我们的证明已简化了许多.

定理 2.7 设 G 是有限 p-群, 若 $\omega(G) < p$, 则 G 正则.

为证明这个定理, 我们先证明两个引理.

引理 2.8 G 是有限非正则 p-群, 但它的每个真子群和真商群都是正则的. (这样的群在文献中称为极小非正则 p-群.) 则有

(1) G 为二元生成;

(2) $\exp G' = p$;

(3) $\mho_1(G) \le Z(G)$.

证 (1) 若 $d(G) > 2$, 则由正则性定义及 G 的极小性知 G 本身正则, 矛盾.

(2) 若 $\mho_1(G') \ne 1$, 则 $G/\mho_1(G')$ 正则. 据定理 2.4, $G/\mho_1(G')$ 又 p-交换, 故对任意 $a, b \in G$, 有

$$b^{-p}a^{-p}(ab)^p \in \mho_1(G').$$

于是存在 $d_1, d_2, \cdots, d_s \in G'$ 使

$$(ab)^p = a^p b^p d_1^p \cdots d_s^p.$$

若 $\langle a, b\rangle = G$, 则对 a, b 已成立正则性条件. 而若 $\langle a, b\rangle < G$, 则由 G 是极小非正则 p-群, $\langle a, b\rangle$ 已经正则, 故 G 是正则的, 矛盾.

(3) 由 (2) 及 G 的真子群正则得 G 的真子群亦 p-交换. 现设 $a, b \in G$, 因 $\langle a, b^{-1}ab\rangle$ 是 G 的真子群, 故 $\langle a, b^{-1}ab\rangle$ p-交换. 于是有

$$[a^p, b] = a^{-p}(b^{-1}ab)^p = (a^{-1}b^{-1}ab)^p = [a, b]^p.$$

又由 (2), $[a, b]^p = 1$, 故 $[a^p, b] = 1$. 最后由 a, b 的任意性, 得 $\mho_1(G) \le Z(G)$. □

引理 2.9 设 G 是有限 p-群, $\omega(G) < p$.
(1) 若 $N \trianglelefteq G$, 则 $\omega(G/N) \leq \omega(G)$;
(2) 若 $H \leq G$, 则 $\omega(H) \leq \omega(G)$.

证 (1) 由定义显然.

(2) 不失普遍性, 可设 H 是 G 的极大子群. 于是 $|G : H| = p$, $H \trianglelefteq G$, 由此又有 $\mho_1(H) \trianglelefteq G$. 现设 $\omega(H) > \omega(G)$, 则由

$$p^{\omega(G)} = |G/\mho_1(G)| < |H/\mho_1(H)| = \frac{1}{p}|G/\mho_1(G)||\mho_1(G)/\mho_1(H)|,$$

得 $|\mho_1(G)/\mho_1(H)| \geq p^2$. 取 $L \trianglelefteq G$ 满足 $\mho_1(H) \leq L < \mho_1(G)$ 且 $|\mho_1(G)/L| = p^2$. 令 $\overline{G} = G/L$, $\overline{H} = H/L$, 则仍有 $\omega(\overline{H}) > \omega(\overline{G})$. 于是若令 G 是使结论不真的最小阶群, 有 $L = 1$, $|\mho_1(G)| = p^2$, $|G| = p^{\omega(G)+2} \leq p^{p+1}$. 我们断言 G 必正则. (若否, 必有 $|G| = p^{p+1}$, 而 G 是极小非正则群, 由引理 2.8(3) 有 $\mho_1(G) \leq Z(G)$, 于是 $|G/Z(G)| \leq p^{p-1}$, $c(G/Z(G)) \leq p-2$, 由此有 $c(G) \leq p-1$, G 正则, 矛盾.) 因 $G' \leq H$, 有 $\mho_1(G') = 1$, 于是 G 又 p-交换. 据定理 2.2(3) 有

$$p^{\omega(H)} = |H/\mho_1(H)| = |\Omega_1(H)| \leq |\Omega_1(G)| = |G/\mho_1(G)| = p^{\omega(G)},$$

得 $\omega(H) \leq \omega(G)$, 矛盾. □

定理 2.7 的证明: 设定理不真, 且设 G 是最小阶反例. 由性质 $\omega(G) < p$ 在取子群和商群下均保持 (引理 2.9), G 是极小非正则群, 于是 $\mho_1(G) \leq Z(G)$(引理 2.8(3)). 因 $p^{\omega(G)} = |G/\mho_1(G)| < p^p$, 有 $c(G/\mho_1(G)) < p-1$, 于是 $c(G/Z(G)) < p-1$, $c(G) < p$, G 正则, 矛盾. 定理证毕. □

§3. 亚交换正则 p-群

称群 G 为亚交换的, 如果 $G'' = 1$. 这时导群 G' 是交换群.

本节主要结果是定理 3.6, 但在证明它之前我们先要建立下列的换位子公式.

定理 3.1 设 G 是亚交换群, $x, y, z \in G$.
(1) 如果 $z \in G'$, 则

$$[z, x]^{-1} = [z^{-1}, x]; \tag{3.1}$$

(2) 如果 $y \in G'$, 则

$$[xy, z] = [x, z][y, z], \tag{3.2}$$

$$[z, xy] = [z, x][z, y]; \tag{3.3}$$

(3) 对任意的 $x, y, z \in G$, 有

$$[x, y^{-1}, z]^y = [y, x, z]; \tag{3.4}$$

(4) 对任意的 $x, y, z \in G$, 有

$$[x, y, z][y, z, x][z, x, y] = 1; \tag{3.5}$$

(5) 如果 $z \in G'$, 则

$$[z, x, y] = [z, y, x]. \tag{3.6}$$

证 (1) 由 IV, 命题 1.2(3) 及 G' 的交换性得

$$[z, x]^{-1} = [z^{-1}, x]^z = [z^{-1}, x].$$

(2) 由 IV, 命题 1.2(4) 和 1.2(5) 及 G' 的交换性立得.
(3) 应用 IV, 命题 1.2 中的诸换位子公式, 得

$$\begin{aligned}[x, y^{-1}, z]^y &= [[x, y^{-1}]^y, z^y] = [[y, x], z[z, y]] \\ &= [y, x, z][[y, x], [z, y]] = [y, x, z].\end{aligned}$$

(4) 由 (3) 及 Witt 公式 (IV, 命题 1.2(6)) 立得.
(5) 由 $z \in G'$ 及 (4) 得

$$[y, z, x][z, x, y] = 1,$$

即 $[z,x,y]=[y,z,x]^{-1}$. 由 (1), $[y,z,x]^{-1}=[[y,z]^{-1},x]=[z,y,x]$, 于是即得 $[z,x,y]=[z,y,x]$. □

由 (3.6) 式用归纳法可得：若 $z\in G'$, $x_1,\cdots,x_n\in G$, 而 σ 是集合 $\{1,2,\cdots,n\}$ 的任一置换, 则有

$$[z,x_1,\cdots,x_n]=[z,x_{1^\sigma},\cdots,x_{n^\sigma}]. \tag{3.7}$$

特别地, 仅由 a,b 二元素作成的任意权的简单换位子中, 除前两项外, 从第三项往后的诸项间次序可以任意调换, 于是总可将其化成 $[a,b,a,\cdots,a,b,\cdots,b]$ 或 $[b,a,\cdots,a,b,\cdots,b]$ 的形状. 设在上述换位子中一共出现了 i 个 a, j 个 b, 其中 i, j 是正整数. 则为简便计, 我们约定

$$[ia,jb]=[a,b,\underbrace{a,\cdots,a}_{i-1},\underbrace{b,\cdots,b}_{j-1}],$$

$$[jb,ia]=[b,\underbrace{a,\cdots,a}_{i},\underbrace{b,\cdots,b}_{j-1}].$$

引理 3.2 设 G 是亚交换群, $a,b\in G$. 又设 m,n 为正整数, 则有

$$[a^m,b^n]=\prod_{i=1}^{m}\prod_{j=1}^{n}[ia,jb]^{\binom{m}{i}\binom{n}{j}}. \tag{3.8}$$

证 对 $m+n$ 用归纳法. 若 $m+n=2$, 公式显然成立. 下面设 $m+n>2$, 这时 m, n 中至少有一个大于 1.

若 $n>1$, 则

$$[a^m,b^n]=[a^m,b][a^m,b^{n-1}]^b.$$

据归纳假设得

$$[a^m,b^n] = \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}\left(\prod_{i=1}^{m}\prod_{j=1}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n-1}{j}}\right)^b$$

$$
\begin{aligned}
&= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}} \cdot \prod_{i=1}^{m}\prod_{j=1}^{n-1}([ia,jb][ia,(j+1)b])^{\binom{m}{i}\binom{n-1}{j}} \\
&= \prod_{i=1}^{m}\left([ia,b]^{\binom{m}{i}}[ia,b]^{\binom{m}{i}\binom{n-1}{1}}[ia,nb]^{\binom{m}{i}}\right. \\
&\quad \left.\cdot\prod_{j=2}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n-1}{j}+\binom{m}{i}\binom{n-1}{j-1}}\right) \\
&= \prod_{i=1}^{m}\left([ia,b]^{\binom{m}{i}\binom{n}{1}}[ia,nb]^{\binom{m}{i}\binom{n}{n}}\prod_{j=2}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n}{j}}\right) \\
&= \prod_{i=1}^{m}\prod_{j=1}^{n}[ia,jb]^{\binom{m}{i}\binom{n}{j}}.
\end{aligned}
$$

而若 $n=1$, 则 $m>1$. 这时有

$$[a^m,b]=[a^{m-1},b]^a[a,b].$$

应用归纳假设得

$$
\begin{aligned}
[a^m,b] &= \left(\prod_{i=1}^{m-1}[ia,b]^{\binom{m-1}{i}}\right)^a [a,b] \\
&= \prod_{i=1}^{m-1}[ia,b]^{\binom{m-1}{i}}\prod_{i=1}^{m-1}[(i+1)a,b]^{\binom{m-1}{i}}\cdot[a,b] \\
&= [a,b][a,b]^{\binom{m-1}{1}}\prod_{i=2}^{m-1}[ia,b]^{\binom{m-1}{i}}\prod_{i=2}^{m}[ia,b]^{\binom{m-1}{i-1}} \\
&= [a,b]^{\binom{m}{1}}\left(\prod_{i=2}^{m-1}[ia,b]^{\binom{m}{i}}\right)[ma,b]^{\binom{m}{m}} \\
&= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}.
\end{aligned}
$$

□

下面的定理给出一个在亚交换群中类似 P. Hall 恒等式的公式.

定理 3.3 设 G 是亚交换群, $a,b\in G, m\geq 2$. 则

$$(ab^{-1})^m = a^m \prod_{i+j\leq m} [ia, jb]^{\binom{m}{i+j}} b^{-m}, \tag{3.9}$$

其中求积号中的 i,j 为正整数, 且满足 $i+j\leq m$.

证 用对 m 的归纳法. 当 $m=2$ 时,

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2b^{-1}[b^{-1},a]bb^{-2} = a^2[a,b]b^{-2},$$

定理成立. 现在设 $m>2$, 由归纳假设有

$$\begin{aligned}(ab^{-1})^m &= (ab^{-1})^{m-1}ab^{-1} \\ &= a^{m-1}\prod_{i+j\leq m-1}[ia,jb]^{\binom{m-1}{i+j}}b^{-m+1}ab^{-1} \\ &= a^{m-1}\prod_{i+j\leq m-1}[ia,jb]^{\binom{m-1}{i+j}}a[a,b^{m-1}]b^{-m} \\ &= a^m\prod_{i+j\leq m-1}[ia,jb]^{\binom{m-1}{i+j}} \\ &\quad\cdot\left(\prod_{i+j\leq m-1}[(i+1)a,jb]^{\binom{m-1}{i+j}}\right)[a,b^{m-1}]b^{-m}.\end{aligned}$$

应用引理 3.2,

$$[a,b^{m-1}] = \prod_{j=1}^{m-1}[a,jb]^{\binom{m-1}{j}},$$

代入上式得

$$(ab^{-1})^m = a^m\prod_{j=1}^{m-2}[a,jb]^{\binom{m-1}{j+1}}\prod_{\substack{i+j\leq m-1\\ i>1}}[ia,jb]^{\binom{m-1}{i+j}}$$

$$
\cdot \prod_{\substack{i+j\le m\\ i>1}} [ia,jb]^{\binom{m-1}{i+j-1}} \prod_{j=1}^{m-1}[a,jb]^{\binom{m-1}{j}} b^{-m}
$$

$$
= a^m \prod_{j=1}^{m-2}[a,jb]^{\binom{m}{j+1}}[a,(m-1)b] \prod_{\substack{i+j\le m-1\\ i>1}} [ia,jb]^{\binom{m}{i+j}}
$$

$$
\cdot \prod_{i+j=m}[ia,jb]\cdot b^{-m}
$$

$$
= a^m \prod_{j=1}^{m-1}[a,jb]^{\binom{m}{j+1}} \prod_{\substack{i+j\le m\\ i>1}} [ia,jb]^{\binom{m}{i+j}} b^{-m}
$$

$$
= a^m \prod_{i+j\le m}[ia,jb]^{\binom{m}{i+j}} b^{-m}.
$$

□

引理 3.4 (Gupta-Newman) 设 G 是亚交换群， $d\in G'$, n 是正整数. 如果 $[d,na]=1$ 对任意的 $a\in G$ 成立, 则对任意的 $a,b\in G$ 成立

$$
[d,b,(n-1)a]^{n!}=1.
$$

证 首先用对 n 的归纳法证明

$$
[d,nab]=[d,na][d,(n-1)a,b]^n[d,na,b]^n\pi_n, \tag{3.10}
$$

其中 π_n 是若干个形如 $[d,ia,jb]$, $i+j\ge n$, $j\ge 2$, 的换位子的乘积. 当 $n=1$ 时,

$$
[d,ab]=[d,a][d,b][d,a,b],
$$

(3.10) 式成立, 其中 $\pi_1=1$. 现在设 $n>1$, 由归纳假设,

$$
[d,(n-1)ab]=[d,(n-1)a][d,(n-2)a,b]^{n-1}[d,(n-1)a,b]^{n-1}\pi_{n-1},
$$

于是

$$\begin{aligned}[d,nab] &= [[d,(n-1)a][d,(n-2)a,b]^{n-1} \\ &\quad \cdot[d,(n-1)a,b]^{n-1}\pi_{n-1},ab] \\ &= [d,(n-1)a,ab][d,(n-2)a,b,ab]^{n-1} \\ &\quad \cdot[d,(n-1)a,b,ab]^{n-1}[\pi_{n-1},ab] \\ &= [d,na][d,(n-1)a,b][d,na,b][d,(n-1)a,b]^{n-1} \\ &\quad \cdot[d,(n-2)a,2b]^{n-1}[d,(n-1)a,2b]^{n-1}[d,na,b]^{n-1} \\ &\quad \cdot[d,(n-1)a,2b]^{n-1}[d,na,2b]^{n-1}[\pi_{n-1},ab] \\ &= [d,na][d,(n-1)a,b]^n[d,na,b]^n\cdot\pi_n,\end{aligned}$$

其中 $\pi_n=[\pi_{n-1},ab][d,(n-2)a,2b]^{n-1}[d,(n-1)a,2b]^{2n-2}[d,na,2b]^{n-1}$, 满足我们的要求, (3.10) 式得证.

下面来证明引理. 对于 $i=0,1,\cdots,n-1$, 令 $f_i=n!/(n-i)!$. 再规定 S_i 代表下述命题: 存在函数 $F_i(a,b)$, 它是若干个形如 $[d,ja,kb]$, $j+k\geq n$, $k\geq i+1$, 的换位子的乘积, 使成立下式

$$[d,(n-i)a,ib]^{f_i}F_i(a,b)=1,\ \forall a,b\in G.$$

容易看出引理的结论等价于命题 S_{n-1} 正确. 而由引理条件立得 S_0 成立. 下面我们将用对 i 的归纳法证明所有的 S_i 皆正确, 于是就证明了引理. 设 $i>0$, 且设 S_{i-1} 正确, 即存在满足条件的 $F_{i-1}(a,b)$ 使

$$[d,(n-i+1)a,(i-1)b]^{f_{i-1}}F_{i-1}(a,b)=1,\ \forall a,b\in G. \tag{3.11}$$

在上式中以 ab 代 a, 得到

$$[d,(n-i+1)ab,(i-1)b]^{f_{i-1}}F_{i-1}(ab,b)=1, \tag{3.12}$$

由 (3.10) 式,

$$\begin{aligned}[d,(n-i+1)ab] &= [d,(n-i+1)a][d,(n-i)a,b]^{n-i-1} \\ &\quad \cdot[d,(n-i+1)a,b]^{n-i+1}\pi,\end{aligned}$$

其中 π 是若干形如 $[d,ja,kb], j+k\geq n-i+1, k\geq 2$, 的换位子的乘积. 代入 (3.12) 式得

$$[d,(n-i+1)a,(i-1)b]^{f_{i-1}}[d,(n-i)a,ib]^{f_i} \cdot[d,(n-i+1)a,ib]^{f_i}[\pi,(i-1)b]F_{i-1}(ab,b)=1. \tag{3.13}$$

由 (3.11) 又得

$$[d,(n-i+1)a,ib]^{f_i}[F_{i-1}(a,b),b]^{n-i+1}=1. \tag{3.14}$$

将 (3.11) 及 (3.14) 代入 (3.13) 得

$$[d,(n-i)a,ib]^{f_i}[\pi,(i-1)b] \cdot F_{i-1}(ab,b)F_{i-1}(a,b)^{-1}[F_{i-1}(a,b),b]^{-(n-i+1)}=1.$$

令 $F_i(a,b)=[\pi,(i-1)b]F_{i-1}(ab,b)F_{i-1}(a,b)^{-1}[F_{i-1}(a,b),b]^{-(n-i+1)}$, 为完成证明只须说明 $F_i(a,b)$ 可表成形如 $[d,ja,kb]$, $j+k\geq n$, $k\geq i+1$, 的换位子的乘积即可. 为此又只须考察 $F_{i-1}(ab,b)\cdot F_{i-1}(a,b)^{-1}$. 而这由 $F_{i-1}(a,b)$ 的性质及 (3.10) 式不难看出, 细节由读者自行补足. □

为叙述下面的引理我们引进下述记号: 设 $N\trianglelefteq G$, 我们以 $a\equiv b(\mathrm{mod}\ N)$ 表 a,b 属于 N 的同一陪集, 即 $aN=bN$.

引理 3.5 设 G 是任意群, n 是正整数. 又设 $a_1,\cdots,a_i,\cdots,a_n,b_i\in G$, $1\leq i\leq n$. 则

(1) $[a_1,\cdots,a_ib_i,\cdots,a_n]\equiv[a_1,\cdots,a_i,\cdots,a_n][a_1,\cdots,b_i,\cdots,a_n]$ $(\mathrm{mod}\ G_{n+1})$;

(2) $[a_1,\cdots,a_i^{-1},\cdots,a_n]\equiv[a_1,\cdots,a_i,\cdots,a_n]^{-1}\quad(\mathrm{mod}\ G_{n+1})$;

(3) 设 $i_1,i_2,\cdots,i_n$ 是任意整数, 则有

$$[a_1^{i_1},\cdots,a_n^{i_n}]\equiv[a_1,\cdots,a_n]^{i_1\cdots i_n}\quad(\mathrm{mod}\ G_{n+1}).$$

证 (1) 由 IV,1.2 中的换位子公式易得

(i) 若 $a,b\in G_i, d\in G$, 则

$$[ab,d]\equiv[a,d][b,d]\pmod{G_{i+2}};$$

(ii) 若 $a,b\in G, d\in G_i$, 则

$$[d,ab]\equiv[d,a][d,b]\pmod{G_{i+2}};$$

(iii) 若 $a\equiv b \pmod{G_{i+1}}$, $d\in G$, 则

$$[a,d]\equiv[b,d]\pmod{G_{i+2}}.$$

应用 (i)–(iii), 对 n 作归纳法来证明所需的结论, 细节略.

(2) 由 (1) 有

$$\begin{aligned} 1 &= [a_1,\cdots,a_ia_i^{-1},\cdots,a_n] \\ &\equiv [a_1,\cdots,a_i,\cdots,a_n][a_1,\cdots,a_i^{-1},\cdots,a_n] \pmod{G_{n+1}}, \end{aligned}$$

由此立得所需之结论.

(3) 由 (2) 可设 $i_1,\cdots,i_n$ 均系正整数. 用对 $i_1+\cdots+i_n$ 的归纳法及 (1) 易得所需之结论, 细节略. □

下面我们将回到正则 p-群的理论, 首先证明关于 p-交换群的一个重要定理 [1].

定理 3.6 设 G 是二元生成的有限亚交换 p-群. 则 G 是 p-交换的当且仅当 $\exp G'\le p$ 并且 $c(G)<p$.

证 充分性: 由 $c(G)<p$ 得 G 正则, 再由 $\exp G'\le p$ 及定理 2.4 得 G 为 p-交换.

必要性: 由定理 2.2(6), 得 $\exp G'\le p$, 即 G' 是初等交换 p-群. 下面用反证法证明 $c(G)<p$. 设结论不真, 并设 G 为最小阶反

[1]这个定理最早由 W. Brisley 和 I.D. Macdonald 在 1969 年发表, 可见他们的论文 “Two classes of metabelian p-groups” (载 *Math. Z*, **112**(1969), 5-12.) 但笔者早在 1964 年也证明了这个定理, 并把它写入毕业论文 “关于有限正则 p-群”§2 中, 即该文的定理 2.2.

例. 则由 G 的最小性有 $c(G)=p$. 因 G 二元生成，可设 $G=\langle a,b\rangle$. 据 IV, 定理 1.8(2), G_p 由换位子 $[x_1,x_2,\cdots,x_p]$ 生成，其中 $x_i=a$ 或 b. 再由定理 3.1(5),

$$G_p=\langle [ia,(p-i)b] \mid i=1,2,\cdots,p-1\rangle.$$

因 $c(G)=p$, 有 $G_p\le Z(G)$. 由定理 3.3 及 $\exp G'\le p$,

$$\begin{aligned}(ab^{-1})^p &= a^p\prod_{i+j\le p}[ia,jb]^{\binom{p}{i+j}}b^{-p}\\ &= a^p\prod_{i=1}^{p-1}[ia,(p-i)b]b^{-p}\\ &= a^pb^{-p}\prod_{i=1}^{p-1}[ia,(p-i)b].\end{aligned}$$

据 p-交换性得

$$\prod_{i=1}^{p-1}[ia,(p-i)b]=1.$$

在上式中以 a^s 代 a, $s=1,2,\cdots,p-1$, 用引理 3.5(3) 得

$$\prod_{i=1}^{p-1}[ia,(p-i)b]^{s^i}=1,\quad s=1,2,\cdots,p-1.$$

如果把它们写成加法形式，可看成是域 $GF(p)$ 上的 $p-1$ 个关于未知数 $[ia,(p-i)b]$, $i=1,\cdots,p-1$, 的齐次线性方程组，其系数行列式是 Vandermonde 行列式

$$\begin{aligned}\Delta &= \begin{vmatrix}1 & 1 & \cdots & 1\\ 2 & 2^2 & \cdots & 2^{p-1}\\ \vdots & \vdots & & \vdots\\ p-1 & (p-1)^2 & \cdots & (p-1)^{p-1}\end{vmatrix}\\ &= 1\cdot 2\cdots(p-1)\prod_{1\le i<j\le p-1}(j-i)\neq 0,\end{aligned}$$

因此只有零解. 即

$$[ia,(p-i)b]=1, i=1,2,\cdots,p-1.$$

由此得 $G_p=1$, $c(G)<p$, 与假设 $c(G)=p$ 矛盾. □

推论 3.7 设 G 是有限亚交换 p-群. 则 G 是 p-交换的当且仅当 $\mho(G')=1$ 且对任一二元生成子群 K 有 $c(K)<p$.

但有例子说明, 亚交换 p-交换 p-群的幂零类可能 $\geq p$.

例 3.8 设 $p=3$, $G=\langle a,b,c\rangle$, 有定义关系: $a^3=b^3=c^3=d_{12}^3=d_{23}^3=d_{31}^3=d^3=1$, $[a,b]=d_{12}$, $[b,c]=d_{23}$, $[c,a]=d_{31}$, $[d_{12},c]=[d_{23},a]=[d_{31},b]=d$, $[d_{12},a]=[d_{12},b]=[d_{23},b]=[d_{23},c]=[d_{31},a]=[d_{31},c]=[d,a]=[d,b]=[d,c]=1$. G 可看成是由 3^4 阶的初等交换 3-群 $A=\langle d_{12},d_{23},d_{31},d\rangle$ 出发, 逐次添加元素 a,b,c 得到. 每次添加相当于一个 3 次循环扩张. 于是 G 是 3^7 阶群, $c(G)=3$. 由计算可得 $\exp G=3$, 于是 G 是 3-交换的. (计算细节留给读者作为习题.)

事实上, 下面定理告诉我们, p 是亚交换 p-交换 p-群幂零类的可能的最大值.

定理 3.9 设 G 是有限亚交换 p-交换 p-群, 则 $c(G)\leq p$.

证 任取 $a_1,a_2,\cdots,a_{p+1}\in G$, 令 $d_2=[a_1,a_2]$. 由 $\langle d_2,a_3\rangle$ p-交换, 应用定理 3.6 得 $[d_2,(p-1)a_3]=1$. 再用引理 3.4, 得

$$[d_2,(p-2)a_4,a_3]^{(p-1)!}=1,\quad \forall a_3,a_4\in G.$$

由 $((p-1)!,p)=1$, 得 $[d_2,a_3,(p-2)a_4]=1$. 令 $d_3=[d_2,a_3]$, 再用引理 3.4, 得

$$[d_3,a_4,(p-3)a_5]^{(p-2)!}=1,\quad \forall a_4,a_5\in G,$$

因 $((p-2)!,p)=1$, 又得 $[d_3,a_4,(p-3)a_5]=1$. 如此反复应用引理 3.4 $p-1$ 次, 即可得到

$$[a_1,a_2,\cdots,a_{p+1}]=1, \quad \forall a_1,a_2,\cdots,a_{p+1}\in G,$$

即 $G_{p+1}=1, c(G)\le p$. □

把定理 3.6 和定理 3.9 应用到亚交换正则 p-群和一般的正则 p-群, 我们得到下面两个定理.

定理 3.10 *设 G 是有限亚交换 p-群. 则*

(1) G 正则的充分必要条件是对 G 的任一二元生成子群 K 成立 $K_p\le \mho_1(K')$.

(2) G 正则的必要条件是 $G_{p+1}\le \mho_1(G')$.

证 (1) 若 G 正则, 则 G 的任一二元生成子群 K 亦正则, 从而 $K/\mho_1(K')$ 正则. 由定理 2.4, $K/\mho_1(K')$ 又 p-交换. 应用定理 3.6, 即得 $K_p\le \mho_1(K')$. 反之, 由 $K_p\le \mho_1(K')$ 及定理 3.6 得 $K/\mho_1(K')$ p-交换, 从而 K 正则, 于是 G 正则.

(2) 由 G 正则得 $G/\mho_1(G')$ p-交换, 定理 3.9 就给出 $c(G/\mho_1(G'))\le p$, 于是 $G_{p+1}\le \mho_1(G')$. □

定理 3.11 *设 G 是有限正则 p-群, 则 $G_{p+1}\le \Phi(G')$; 又若 $d(G)=2$, 则 $G_p\le \Phi(G')$.*

证 由 G 正则得 $G/\mho_1(G')$ p-交换. 因 $\Phi(G')=\mho_1(G')G''$, 又得 $G/\Phi(G')$ 为亚交换 p-交换群. 于是定理 3.6 和定理 3.9 即给出所需的结论. □

应用定理 3.11, 我们可给下面关于正则 2-群和正则 3-群的著名结果一个简短的新证明.

定理 3.12 *(1) 正则 2-群是交换的;*

(2) 二元生成有限 3-群 G 正则的充要条件为 G' 循环.

证 (1) 设 G 是正则 2-群, $a, b \in G$. 令 $K = \langle a, b \rangle$. 由定理 3.11 有 $K_2 = K' \le \Phi(K')$, 这迫使 $K' = 1$, 即 a, b 可交换. 由 a, b 的任意性即得 G 交换.

(2) 只须证必要性. 由 G 正则及定理 3.11 得 $G_3 \le \Phi(G')$. 据 IV, 定理 1.8(4), 若 $G = \langle a, b \rangle$, 则

$$G' = \langle G_3, [a, b] \rangle.$$

由 $G_3 \le \Phi(G')$ 即得 $G' = \langle [a, b] \rangle$, 从而 G' 循环. □

更进一步, 我们还可将定理 3.12 推广为

定理 3.13 *设 G 是有限正则 p-群, $d(G) = 2$. 则 $d(G') \le \frac{(p-1)(p-2)}{2}$, 并且等号是可以达到的.*

证 设 $G = \langle a, b \rangle$, 不失普遍性, 还可设 G' 为初等交换 p-群. 于是由定理 3.6 有 $c(G) < p$. 据 IV, 定理 1.8(2) 及本章定理 3.1(5) 易看出

$$G' = \langle [ia, jb] \mid 2 \le i + j \le p - 1, i \ge 1, j \ge 1 \rangle,$$

故 $|G'| \le p^{1+2+\cdots+(p-2)} = p^{\frac{1}{2}(p-1)(p-2)}$, 即 $d(G') \le \frac{1}{2}(p-1)(p-2)$.

为了说明等号可以达到, 我们给出下例: $G = \langle a, b \rangle$, 其定义关系为: $a^p = b^p = 1$; $[ia, jb] = d_{ij}$, 若 $i, j \ge 1$ 且 $i + j \le p - 1$; $[ia, jb] = 1$, 若 $i + j \ge p$; $d_{ij}^p = 1$, $[d_{ij}, d_{kl}] = 1$, $i, j, k, l \ge 1$, $i + j \le p - 1$, $k + l \le p - 1$. 事实上, G 可看成由 $p^{\frac{1}{2}(p-1)(p-2)}$ 阶初等交换群 $A = \langle d_{ij} \mid i, j \ge 1, i + j \le p - 1 \rangle$ 作两次循环扩张得到 (依次添加元素 a 和 b). 并容易验证 $|G| = p^{2+\frac{1}{2}(p-1)(p-2)}$, 且 $G' = A$, $|G'| = p^{\frac{1}{2}(p-1)(p-2)}$, 于是 $d(G') = \frac{1}{2}(p-1)(p-2)$; 又 $c(G) = p - 1$, 于是 G 是正则的. 这样 G 是我们所需的使等号达到的例子. □

最后我们谈一下关于正则 p-群的直积的问题. H. Wielandt 最早指出, 如果 $p > 2$, 两个正则 p-群的直积不一定正则. 他给出了一个例子. 后来, O. Grün, P.M. Weichsel 和 J.R.J. Groves 都研究了这个问题, 下面我们来叙述他们的主要结果.

定理 3.14 设 G 是有限正则 p-群. 则 G 与任何有限正则 p-群 H 的直积 $G\times H$ 均正则的充分必要条件为 G 是 p-交换群.

证 由于正则 2-群必 2-交换, 故此定理对 $p=2$ 的情形显然成立. 下面设 $p>2$.

充分性: 设 G p-交换, H 正则. 令 $D=G\times H$, 我们要证明 D 也正则. 任给 $d_1,d_2\in D$. 设 $d_i=g_ih_i$, $g_i\in G$, $h_i\in H$, $i=1,2$. 因为 G p-交换, H 正则, 有

$$\begin{aligned}(g_1g_2)^p &= g_1^pg_2^p,\\(h_1h_2)^p &= h_1^ph_2^pc_1^p\cdots c_s^p,\ c_i\in\langle h_1,h_2\rangle'.\end{aligned}$$

于是

$$\begin{aligned}(d_1d_2)^p &= (g_1g_2)^p(h_1h_2)^p=g_1^pg_2^ph_1^ph_2^pc_1^p\cdots c_s^p\\&= d_1^pd_2^pc_1^p\cdots c_s^p.\end{aligned}$$

因 $c_i\in\langle h_1,h_2\rangle'$, c_i 总可表成有限多个形如 $[s,t]$ 的换位子的乘积, 其中 $s,t\in\langle h_1,h_2\rangle$, 于是 s,t 可表成由 h_1,h_2 组成的有限积. 在这些乘积式中我们以 d_1,d_2 去代替 h_1,h_2, 得到 s',t', 易看出 $s'=ss''$, $t'=tt''$, 其中 $s'',t''\in\langle g_1,g_2\rangle$. 经过这样的代换如果 c_i 变成了 x_i, 则 $x_i=c_iy_i$, 其中 $y_i\in\langle g_1,g_2\rangle'$. 因为 G p-交换, 有 $x_i^p=c_i^py_i^p=c_i^p$, 故由上式得到

$$(d_1d_2)^p=d_1^pd_2^px_1^p\cdots x_s^p,x_i\in\langle d_1,d_2\rangle',$$

于是 D 正则.

必要性: 设 G 正则但非 p-交换, 我们要找一个正则 p-群 H 使 $D=G\times H$ 不正则.

首先如下构造 H: 设

$$A=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_{p-1}\rangle,$$

其中 $o(a_1)=o(a_2)=p^2$, 但对 $i>2$, $o(a_i)=p$. 规定映射 β :

$$\begin{aligned}a_i^\beta &= a_ia_{i+1}, i=1,2,\cdots,p-2,\\a_{p-1}^\beta &= a_{p-1}a_2^{\binom{p}{2}},\end{aligned}$$

再把它扩充到整个 A 上. 易验证 β 是 A 的 p^2 阶自同构. 令 $H = A \rtimes \langle b\rangle$, $o(b) = p^2$, 且 b 在 A 上的作用与 β 相同. 我们要证明 H 即符合我们的要求.

首先易验证 $H = \langle a_1, b\rangle$, $H' = \langle a_2\rangle \times \cdots \times \langle a_{p-1}\rangle$, $H_3 = \langle a_2^p\rangle \times \langle a_3\rangle \times \cdots \times \langle a_{p-1}\rangle$, $H_4 = \langle a_2^p\rangle \times \langle a_4\rangle \times \cdots \times \langle a_{p-1}\rangle, \cdots$, $H_p = \langle a_2^p\rangle$, $c(H) = p$. 因 $\exp H' = p^2$, 故 H 非 p-交换. 但因 $\mho_1(H') \geq H_p$, 易推知 H 正则. 注意到 $\exp H_3 = p$, 我们用定理 3.3 来计算 $(a_1b)^p$:

$$\begin{aligned}(a_1b)^p &= a_1^p \prod_{i+j\leq p} [ia_1, jb^{-1}]^{\binom{p}{i+j}} b^p \\ &= a_1^p [a_1, b^{-1}]^{\binom{p}{2}} [a_1, (p-1)b^{-1}] b^p.\end{aligned}$$

因

$$[a_1, b^{-1}] = ([a_1, b]^{b^{-1}})^{-1} = (a_2[a_2, b^{-1}])^{-1} = a_2^{-1}[a_2, b^{-1}]^{-1},$$

故

$$[a_1, b^{-1}]^{\binom{p}{2}} = a_2^{-\binom{p}{2}}[a_2, b^{-1}]^{-\binom{p}{2}} = a_2^{-\binom{p}{2}}.$$

又因 $c(H) = p$, 用引理 3.5(3) 得

$$[a_1, (p-1)b^{-1}] = [a_1, (p-1)b]^{(-1)^{p-1}} = [a_1, (p-1)b] = a_2^{\binom{p}{2}},$$

于是得 $(a_1b)^p = a_1^p b^p$.

下面用上述关于 H 的事实证明 $D = G \times H$ 不正则. 不失普遍性, 可假定 G 是极小非 p-交换群, 即 G 非 p-交换, 但 G 的每个真子群和真商群均 p-交换. 这时有 $G = \langle g, h\rangle$ 是二元生成的, 且可设 $(gh)^p \neq g^p h^p$. 设 $M \leq Z(G)$, 且 $|M| = p$. 则 $M \trianglelefteq G$, 且 G/M p-交换. 于是 $[g, h]^p \in M$, 再设 k 是 G 之任意元素, 由 $[[g, h]^p, k] = 1$ 及 G 之正则性, 有 $[g, h, k]^p = 1$, 即 $G_3 \leq \Omega_1(G)$. 再由 G 正则的定义, 有

$$(gh)^p = g^p h^p [g, h]^{pr},$$

其中 $p \nmid r$, 而 $[g, h]$ 的阶恰为 p^2. 令 $x = ga_1, y = hb$, 我们要证 $\langle x, y\rangle$ 不正则. 若否, 则由 $G_3 \leq \Omega_1(G)$, $H_3 \leq \Omega_1(H)$, 有 $D_3 \leq \Omega_1(D)$, 于

是有

$$(xy)^p = x^p y^p [x,y]^{ps}, s\text{是整数}.$$

但 $(xy)^p = (ga_1hb)^p = (gh)^p(a_1b)^p = g^p h^p [g,h]^{pr} a_1^p b^p = x^p y^p [g,h]^{pr}$, 于是 $[g,h]^{pr} = [x,y]^{ps} = [g,h]^{ps}[a_1,b]^{ps}$. 由此得 $[a_1,b]^{ps} = 1$. 因 $[a_1,b]$ 的阶为 p^2, 故 $p \mid s$. 于是 $[g,h]^{pr} = [g,h]^{ps}[a_1,b]^{ps} = 1$, 与 $[g,h]^{pr} \neq 1$ 矛盾. □

§4.　正则 p-群的幂结构

在 §2 开头处我们定义了有限 p-群的上、下幂群列. 与其紧密相关的是如下定义的 p-群的幂映射：设 G 是有限 p-群， s 是正整数， G 的 s 次幂映射π_s 用下式规定：

$$\pi_s : a \mapsto a^{p^s}, \quad \forall a \in G.$$

我们所谓 p-群的 “幂结构” 指的就是 p-群的上、下幂群列及幂映射的性质. 对于正则 p-群来说，它们的幂结构有很好的性质，很多方面类似于交换 p-群. 甚至正则 p-群也有类似于交换 p-群的基底 ——所谓唯一性基底. 事实上， P. Hall 对正则 p-群的研究主要就集中在它们的幂结构性质上. 正则 p-群幂结构最主要的性质是定理 2.6. 用幂映射的性质来写即下面的

定理 4.1 设 G 是有限正则 p-群， π_s 是它的 s 次幂映射. 则

(1) $\mathrm{Ker}\ \pi_s = \Omega_s(G), \mathrm{Im}\ \pi_s = \mho_s(G)$;

(2) 映射 $\bar{\pi}_s : a\Omega_s(G) \mapsto a^{p^s}$, $\forall a \in G$, 是 $G/\Omega_s(G)$ 到 $\mho_s(G)$ 上的一一映射，特别地， $|G/\Omega_s(G)| = |\mho_s(G)|$.

我们说这个定理是正则 p-群幂结构的基本性质，原因是如果我们假定有限 p-群 G 的每个截段 (即子群的商群) 都满足定理 2.6 或定理 4.1 的性质，则 G 必为正则的. 事实上，我们可以在下面更弱的条件下证明这个结果.

称有限 p-群 G 为半 p-交换的，如果对任意的 $a, b \in G$, 有 $(a^{-1}b)^p = 1$ 当且仅当 $a^p = b^p$. 事实上，这个条件仅对应于定理 2.6(2) 中 $s = 1$ 的情形. 我们有

定理 4.2 有限 p-群 G 正则的充要条件是 G 的每个截段半 p-交换.

证 设 G 是使定理不真的最小阶反例，则 G 是极小非正则 p-群. 由引理 2.8 知 G 为二元生成，且 $\exp G' = p$, $\mho_1(G) \le Z(G)$. 由定理 2.4 又得 G 的每个真截段非但是正则的而且是 p-交换的，即 G 是极小非 p-交换群. 这时我们断言 $Z(G)$ 必为循环群. 若否，取 $Z(G)$ 中二不同的 p 阶子群 M 和 N, 由 G/M 和 G/N p-交换及 G 同构于 $(G/M)\times(G/N)$ 的子群得 G p-交换，矛盾. 故 $Z(G)$ 循环，于是 $\mho_1(G)$ 也循环.

现在任取 G 的一组生成元 a, b, 不妨设 $o(a) \ge o(b)$. 由 $a^p, b^p \in \mho_1(G)$, 存在正整数 m 使 $a^{mp} = b^p$. 由半 p-交换性得 $(ba^{-m})^p = 1$. 令 $b' = ba^{-m}$, 则 $G = \langle a, b'\rangle$. 因 $b' \in \Omega_1(G)$ 有 $G = \langle a, \Omega_1(G)\rangle$, 故 G 中任一元均可表成 $a^i x$ 的形状，其中 $x \in \Omega_1(G)$. 任取 G 的二元素 $a^i x$, $a^j y$, 其中 $x, y \in \Omega_1(G)$. 我们有

$$\begin{aligned}(a^i x a^j y)^p &= (a^{i+j}x[x,a^j]y)^p = a^{(i+j)p} = a^{ip}a^{jp}\\ &= (a^i x)^p (a^j y)^p,\end{aligned}$$

于是 G 是 p-交换的，与 G 为反例矛盾. □

这个定理可以作为正则 p-群的另一定义，它是纯粹用 p-群的幂结构性质来刻划正则性的.

注 4.3 A. Mann 在 "The power structure of p-groups I" (载 *J. Algebra* **42**(1976), 121-135) 一文中对 p-群的幂结构性质做了有趣的研究. 他假定有限 p-群 G 的每个截段 K 都具有下列三个性质中的一个:

(1) $\mathrm{Im}\ \pi_s|_K = \mho_s(K)$;

(2) $\mathrm{Ker}\ \pi_s|_K = \Omega_s(K)$;

(3) $|K/\Omega_s(K)| = |\mho_s(K)|$,

但不假定映射 π_s 是 $K/\Omega_s(K)$ 到 $\mho_s(K)$ 上的一一映射，这时推不出 G 是正则的. 由此看出定理 4.1(2) 描述的性质是正则 p-群很基本的性质. 该文中还有大量关于 p-群幂结构的有趣结果.

下面我们定义正则 p-群的一组不变量.

定义 4.4 设 G 是有限正则 p-群, $\exp G = p^e$. 对于 $1 \le s \le e$, 令

$$p^{\omega_s(G)} = |\Omega_s(G)/\Omega_{s-1}(G)|,$$

称 $(\omega_1, \omega_2, \cdots \omega_e)$ 为 G 的 ω-不变量, 其中 $\omega_s = \omega_s(G)$.

命题 4.5 (1) $p^{\omega_s} = |\mho_{s-1}(G)/\mho_s(G)|, s = 1, 2, \cdots, e$;

(2) $\omega_1 = \omega \ge \omega_2 \ge \cdots \ge \omega_e > 0$.

证 (1) 由定理 4.1(2), $|G/\Omega_s(G)| = |\mho_s(G)|$. 由此立得结论.

(2) 由 (1), $p^{\omega_1(G)} = |G/\mho_1(G)| = p^{\omega(G)}$, 故 $\omega_1 = \omega$. 又对任意的 s, $1 \le s \le e$, $\Omega_s(G) \ne \Omega_{s-1}(G)$, 故 $\omega_s > 0$. 最后证明 $\omega_s \ge \omega_{s+1}$. 因为

$$\begin{aligned} p^{\omega_s} &= |\Omega_s(G)/\Omega_{s-1}(G)| = |\Omega_1(G/\Omega_{s-1}(G))| \\ &= |(G/\Omega_{s-1}(G))/\mho_1(G/\Omega_{s-1}(G))| = |G/\mho_1(G)\Omega_{s-1}(G)|. \end{aligned}$$

同理, $p^{\omega_{s+1}} = |G/\mho_1(G)\Omega_s(G)|$. 因 $\Omega_s(G) \ge \Omega_{s-1}(G)$, 故得 $\omega_s \ge \omega_{s+1}$, 证毕. □

上述命题又允许我们定义正则 p-群的另一组不变量, 叫做型不变量. 它很类似于交换 p-群的型不变量.

定义 4.6 对于任意的正整数 i, $1 \le i \le \omega$, 令 e_i 为在集合 $\{\omega_1, \omega_2, \cdots, \omega_e\}$ 中 $\ge i$ 的元素个数, 这样得到一组正整数 $e_1 \ge e_2 \ge \cdots \ge e_\omega$, 称它们为 G 的 e-不变量, 或型不变量, 记作 $(e_1, e_2, \cdots, e_\omega)$.

如果 G 是交换 p-群, 当然它也是正则的. 这时, 上面定义的型不变量即交换 p-群的型不变量, 这点留给读者去证明. 另外, 在正则 p-群的 ω-不变量和 e-不变量之间存在对偶的关系. 即 ω_s 也恰为在集合 $\{e_1, e_2, \cdots, e_\omega\}$ 中 $\ge s$ 的元素个数, 它的证明也留

给读者. 为了更容易看清两组不变量之间的关系, 我们如下定义正则 p-群 G 的型矩阵 $F(G)=(f_{ij}(G))_{e\times\omega}$, 它是 e 行 ω 列的长方矩阵, 其中

$$f_{ij}(G)=\begin{cases}1, & 若 j\le\omega_i,\\ 0, & 若 j>\omega_i.\end{cases}$$

容易看出 F 的第 i 行前 ω_i 个元素为 1, 第 j 列的前 e_j 个元素为 1, 其余均为 0.

与交换群类似, 我们有

命题 4.7 设 G 是有限正则 p-群.

(1) 若 $H\le G$, 则对一切有意义的 i,j 有

$$\omega_i(H)\le\omega_i(G),\ e_j(H)\le e_j(G),\ f_{ij}(H)\le f_{ij}(G);$$

(2) 若 $N\trianglelefteq G$, $\overline{G}=G/N$. 则对一切有意义的 i,j 有

$$\omega_i(\overline{G})\le\omega_i(G),\ e_j(\overline{G})\le e_j(G),\ f_{ij}(\overline{G})\le f_{ij}(G).$$

证 首先容易看出, 三组关系式中只须证明第一组即可.

先看 $i=1$ 的情形. 由 $H\le G$ 显然有 $\Omega_1(H)\le\Omega_1(G)$, 于是得 $\omega_1(H)\le\omega_1(G)$. 又若 $N\trianglelefteq G$, 由

$$\begin{aligned}|\Omega_1(G/N)| &= |(G/N)/\mho_1(G/N)|=|(G/N)/(\mho_1(G)N/N)|\\ &= |G/(\mho_1(G)N)|\le|G/\mho_1(G)|=|\Omega_1(G)|,\end{aligned}$$

得 $\omega_1(G/N)\le\omega_1(G)$, 即 $\omega_1(\overline{G})\le\omega_1(G)$.

而若 $i>1, H\le G$, 由

$$\begin{aligned}|\Omega_1(H/\Omega_{i-1}(H))| &= |\Omega_1(H/H\cap\Omega_{i-1}(G))|\\ &= |\Omega_1(H\Omega_{i-1}(G)/\Omega_{i-1}(G)|\\ &\le |\Omega_1(G/\Omega_{i-1}(G)|,\end{aligned}$$

得 $\omega_i(H)\le\omega_i(G)$. 商群的情况可类似证明, 从略. □

对于型不变量为 $(e_1,e_2,\cdots,e_\omega)$ 的交换 p-群 G 及任一组正整数 $e_1'\ge e_2'\ge\cdots\ge e_{\omega'}'$, 只要 $\omega'\le\omega$, $e_j'\le e_j$, 都存在 G 的子群和商

群，以 $(e'_1, e'_2, \cdots, e'_{\omega'})$ 为其型不变量. 但对于正则 p-群，这个性质不一定成立.

例 4.8 设 $p > 2, G = \langle a, b\rangle$, 有定义关系： $a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = [c, b] = 1$.

因 $G' = \langle c\rangle$ 循环，$p > 2$, 知 G 正则，其型不变量为 $(2, 2, 1)$, 但 G 中没有型不变量为 $(2, 2)$ 的子群. 若否，G 有这样的子群 H, 则因 H 是 G 的极大子群，$G' \le H$. 因 $|G'| = p$, 故 $G' \le \Omega_1(H)$. 由 H 的型不变量为 $(2, 2)$, $\Omega_1(H) = \mho_1(H)$, 故 $G' \le \mho_1(H) \le \mho_1(G)$, 于是 $\Phi(G) = \mho_1(G)$. 因 $|G/\Phi(G)| = p^2$, 而 $|G/\mho_1(G)| = |\Omega_1(G)| = p^3$, 矛盾.

例 4.9 设 $p > 2$, G 为方次数 p^2 的 p^3 阶非交换群，即 $G = \langle a, b\rangle$, 有定义关系： $a^{p^2} = b^p = 1$, $b^{-1}ab = a^{1+p}$. 显然 G 为正则 p-群，其型不变量为 $(2, 1)$, 但它设有型不变量为 (2) 的商群. 若否，则 G 有 p 阶正规子群 N 使 G/N 为 p^2 阶循环群. 因 $N \le Z(G)$, 则 G 必交换，与 G 非交换矛盾.

探索什么样的正则 p-群才能具有一切可能的型不变量的子群和商群，这是一个饶有趣味的问题，但在这方面目前还很少有成果.

下面我们证明正则 p-群的唯一性基底定理.

定义 4.10 有限群 G 的有序元素组 $(b_1, b_2, \cdots, b_r)$, 其诸元素的阶 $o(b_i) = n_i > 1$, $i = 1, 2, \cdots, r$ 被称为是 G 的一组**唯一性基底**, 如果对任意的 $g \in G$, g 均可唯一表成下列形式:

$$g = b_1^{m_1} b_2^{m_2} \cdots b_r^{m_r}, \qquad 0 \le m_i < n_i, \quad i = 1, 2, \cdots, r.$$

引理 4.11 *若有限正则 p-群 G 有唯一性基底 $(b_1, b_2, \cdots, b_r)$, 则 $r = \omega(G)$, 且将 $\{o(b_i) \mid i = 1, 2, \cdots, r\}$ 排成降序必为 $p^{e_1}, p^{e_2}, \cdots, p^{e_\omega}$, 这里 $(e_1, e_2, \cdots, e_\omega)$ 是 G 的型不变量.*

证 设 $A=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_r\rangle$ 是以 $(a_1,a_2,\cdots,a_r)$ 为基底的交换 p-群，满足 $o(a_i)=o(b_i), i=1,2,\cdots,r$. 为证明引理，只须证 G 和 A 有相同的型不变量. 而这又只须证明对任意的 s, 有 $|\mho_s(G)|=|\mho_s(A)|$, 从而 G 和 A 有相同的 ω-不变量.

考虑映射 $f: g=b_1^{m_1}\cdots b_r^{m_r}\mapsto h=a_1^{m_1}\cdots a_r^{m_r}$, $0\le m_i<n_i$, $i=1,2,\cdots,r$. 易见 f 是 G 到 A 上的一一映射. 对任意的 $h=a_1^{m_1}\cdots a_r^{m_r}\in\mho_s(A)$(或 $\Omega_s(A)$), 我们有 $p^s\mid m_i$(或 $n_i\mid p^s m_i$), 于是由定理 2.6 有 $f^{-1}(h)\in\mho_s(G)$. 这说明 $|\mho_s(G)|\ge|\mho_s(A)|$, $|\Omega_s(G)|\ge|\Omega_s(A)|$. 但因

$$|\mho_s(G)||\Omega_s(G)|=|G|=|A|=|\mho_s(A)||\Omega_s(A)|,$$

必有 $|\mho_s(G)|=|\mho_s(A)|$ 及 $|\Omega_s(G)|=|\Omega_s(A)|$, 引理得证. □

为了证明唯一性基底的存在性，我们再引进下面的

定义 4.12 设 G 是有限正则 p-群，令

$$W_i(G)=\mho_1(G)\Omega_i(G),\ i=0,1,\cdots,e=e(G).$$

称群列

$$\mho_1(G)=W_0(G)\le W_1(G)\le\cdots\le W_{e-1}(G)<W_e(G)=G \quad (W)$$

为 G 的 *W-群列*.

在 W-群列中去掉重复项，再任意加细成 G 到 $\mho_1(G)$ 间的一个主群列

$$G=L_0(G)>L_1(G)>\cdots>L_\omega(G)=\mho_1(G), \qquad (L)$$

叫做 G 的一个 *L-群列*.

引理 4.13 *设 (W) 和 (L) 分别为正则 p-群 G 的 W-群列和一个 L-群列. 则对任意的 $i=0,1,\cdots,e-1$, 有 $W_i(G)=L_{\omega_{i+1}}(G)$.*

证　因为

$$\begin{aligned} p^{\omega(G/\Omega_i(G))} &= |G/\Omega_i(G):\mho_1(G/\Omega_i(G))| \\ &= |G:\mho_1(G)\Omega_i(G)| \\ &= |G:W_i(G)|, \end{aligned}$$

又 $p^{\omega(G/\Omega_i(G))}=|\Omega_{i+1}(G):\Omega_i(G)|=p^{\omega_{i+1}(G)}$, 故 $|G:W_i(G)|=p^{\omega_{i+1}}$. 而 $|G:L_{\omega_{i+1}}(G)|=p^{\omega_{i+1}}$, 故 $W_i(G)=L_{\omega_{i+1}(G)}$. □

定理 4.14 (P. Hall) 设 (L) 是有限正则 p-群 G 之任一 L-群列. 取 b_i 是 $L_{i-1}(G)\setminus L_i(G)$ 中任一最小阶元素, $i=1,2,\cdots,\omega$, 则 $(b_1,b_2,\cdots,b_\omega)$ 是 G 的一组唯一性基底.

证　首先证明 $o(b_i)=p^{e_i}$, $i=1,2,\cdots,\omega$. 令 α 是满足 $\omega_{\alpha+1}<i\le\omega_\alpha$ 的正整数, 由型不变量的定义有 $e_i=\alpha$. 因此我们只要证明 $o(b_i)=p^\alpha$ 即可. 由 $\omega_{\alpha+1}<i\le\omega_\alpha$ 有 $L_{\omega_{\alpha+1}}>L_i\ge L_{\omega_\alpha}$, 即 $W_\alpha>L_i\ge W_{\alpha-1}$. 由此又有 $W_\alpha\ge L_{i-1}>L_i\ge W_{\alpha-1}$. 因所有阶 $\le p^{\alpha-1}$ 的元素 (它们组成子群 $\Omega_{\alpha-1}(G)$) 都属于 $W_{\alpha-1}$, 故 $L_{i-1}\setminus L_i$ 中元素的阶均 $\ge p^\alpha$. 但由 $W_\alpha=W_{\alpha-1}\Omega_\alpha$, W_α 可由 $W_{\alpha-1}$ 及所有 p^α 阶元素生成, 于是对任意的 $g\in W_\alpha$, 有 $g=hk$, 其中 $h\in W_{\alpha-1}$, k 是 p^α 阶元. 设 $L_{i-1}=\langle L_i,g\rangle$, 由 $g\in L_{i-1}$ 得 $k\in L_{i-1}$, 又 $k\notin L_i$, 故 $k\in L_{i-1}\setminus L_i$, 于是 $L_{i-1}\setminus L_i$ 中确有 p^α 阶元, 这就证明了 $o(b_i)=p^\alpha$.

下面对 $|G|$ 用归纳法证明 $(b_1,b_2,\cdots,b_\omega)$ 是 G 的唯一性基底. 如果 $e=1$, 即 $\exp G=p$, 这时 (L) 群列是 G 的主群列, 显然 $(b_1,b_2,\cdots,b_\omega)$ 是 G 的一组唯一性基底. 下面设 $e>1$, 并设 $o(b_i)=p^e$, $i=1,2,\cdots,s$, 但 $o(b_{s+1})<p^e$, 如果 $s<\omega$ 的话. 这时有 $L_s(G)=\langle\mho_1(G),b_{s+1},\cdots,b_\omega\rangle\le\Omega_{e-1}(G)$, 而 $L_{s-1}(G)\not\le\Omega_{e-1}(G)$. 于是 $\Omega_{e-1}(L_{s-1})\ge L_s$, 但 $L_{s-1}\ne\Omega_{e-1}(L_{s-1})$. 因 $|L_{s-1}:L_s|=p$, 有 $\Omega_{e-1}(L_{s-1})=L_s$. 由此得

$$\omega_e(L_{s-1})=\omega(L_{s-1}/\Omega_{e-1}(L_{s-1}))=\omega(L_{s-1}/L_s)=1.$$

据定理 4.1, $|\mho_{e-1}(L_{s-1})|=p^{\omega_e(L_{s-1})}=p$. 因为 $1\ne b_s^{p^{e-1}}\in\mho_{e-1}(L_{s-1})$, 故 $\langle b_s^{p^{e-1}}\rangle=\mho_{e-1}(L_{s-1})\trianglelefteq G$. 于是 $b_s^{p^{e-1}}\in Z(G)$.

现在作商群 $\overline{G} = G/\mho_{e-1}(L_{s-1}) = G/\langle b_s^{p^{e-1}}\rangle$. 因为 $b_s^{p^{e-1}} \in \mho_1(G) = W_0(G)$, 故 $b_s^{p^{e-1}} \in L_i$, $i = 0, 1, \cdots, \omega$. 令 $\overline{L}_i = L_i/\langle b_s^{p^{e-1}}\rangle$, 得到群列

$$\overline{G} = \overline{L}_0 > \overline{L}_1 > \cdots > \overline{L}_\omega = \mho_1(\overline{G}) = \mho_1(G)/\langle b_s^{p^{e-1}}\rangle.$$

我们要证 $(\overline{L})$ 仍为 $\overline{G}$ 之一 L-群列, 并且 $\bar{b}_i = b_i\langle b_s^{p^{e-1}}\rangle$ 仍为 $\overline{L}_{i-1}\backslash\overline{L}_i$ 中的最小阶元素, 且对于 $i \neq s$ 有 $o(\bar{b}_i) = o(b_i)$, 但 $o(\bar{b}_s) = p^{e-1}$. 证明了这点就可用归纳假设得 $(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_\omega)$ 是 $\overline{G}$ 的唯一性基底, 于是对任意的 $\bar{g} \in \overline{G}$, 可唯一表成

$$\bar{g} = \bar{b}_1^{m_1}\bar{b}_2^{m_2}\cdots\bar{b}_\omega^{m_\omega}, \quad 0 \leq m_i < p^{e_i}, \quad i \neq s, \text{但} 0 \leq m_s < p^{e-1}$$

的形状. 由此对任一 $g \in G$, 可唯一表成

$$\begin{aligned} g &= b_1^{m_1}b_2^{m_2}\cdots b_\omega^{m_\omega}\cdot b_s^{kp^{e-1}} \\ &= b_1^{m_1}b_2^{m_2}\cdots b_s^{m_s+kp^{e-1}}\cdots b_\omega^{m_\omega}, \quad 0 \leq m_i < p^{e_i}, \\ &\qquad i \neq s,\ 0 \leq m_s + kp^{e-1} < p^e \end{aligned}$$

的形状, 即 $(b_1, b_2, \cdots, b_\omega)$ 是 G 的唯一性基底.

下面先证明若 $i \neq s$, 则 $\overline{G}\setminus\overline{L}_i$ 中任一元 $\bar{x}$ 的阶均 $\geq o(b_i)$. 首先对 $\bar{x}$ 的原象 x 有 $o(x) \geq o(b_i)$, 于是 $o(\bar{x}) \geq o(b_i)/p$. 若 $o(\bar{x}) = o(b_i)/p$, 则 $x^{p^{e_i-1}} \in \langle b_s^{p^{e-1}}\rangle$, 可设 $x^{p^{e_i-1}} = b_s^{jp^{e-1}}$. 由定理 2.6 得 $(xb_s^{-jp^{e-e_i}})^{p^{e_i-1}} = 1$. 如果 $i > s$, 有 $e - e_i > 0$. 因 $b_s^{-jp^{e-e_i}} \in \mho_1(G) \leq L_i$, 故 $xb_s^{-jp^{e-e_i}} \in G \setminus L_i$. 但其阶 $< o(b_i)$, 与 b_i 的取法矛盾. 而若 $i < s$, 有 $e = e_i$ 且 $b_s^{-j} \in L_i$. 由此亦得到 $xb_s^{-j} \in G \setminus L_i$. $o(xb_s^{-j}) < o(b_i)$, 与 b_i 的取法矛盾, 结论得证. 第二步, 我们注意, 若 $i = s$, $\overline{G}\setminus\overline{L}_s$ 中确有 p^{e-1} 阶元素 $\bar{b}_s$, 它在 $\overline{L}_{s-1}\setminus\overline{L}_s$ 中, 但 $\overline{G}\setminus\overline{L}_{s-1}$ 中所有元素均为 p^e 阶的. 这说明 $W_{e-1}(\overline{G}) = \overline{L}_{s-1}$, 而对 $j \neq e-1$, 仍有 $W_j(\overline{G}) = \overline{W_j(G)}$, 是 $(\overline{L})$ 中的一项. 故由 L-链的定义知 $(\overline{L})$ 是 $\overline{G}$ 的一个 L-群列, 且 $\bar{b}_i$ 是 $\overline{L}_{i-1}\setminus\overline{L}_i$ 中的最小阶元素. 定理完全证毕. □

应该注意, 上述定理的逆不真. 即存在非正则 p-群也有唯一性基底. 最简单的例子是 8 阶二面体群.

下面的定理给出有限正则 p-群的上、下幂群列与上、下中心群列之间的关系.

定理 4.15 设 G 是有限正则 p-群, $a,b\in G$, s,t 是正整数, 则 $[a^{p^s},b^{p^t}]=1$ 当且仅当 $[a,b]^{p^{s+t}}=1$.

证 由定理 2.6 有

$$\begin{aligned}
& [a^{p^s},b^{p^t}]=(a^{-p^s}(b^{-p^t}ab^{p^t})^{p^s})=1\\
\Longleftrightarrow\quad & (a^{-1}b^{-p^t}ab^{p^t})^{p^s}=1\\
\Longleftrightarrow\quad & ((a^{-1}b^{-1}a)^{p^t}b^{p^t})^{p^s}=1\\
\Longleftrightarrow\quad & (a^{-1}b^{-1}a)^{p^{s+t}}b^{p^{s+t}}=1\\
\Longleftrightarrow\quad & (a^{-1}b^{-1}ab)^{p^{s+t}}=[a,b]^{p^{s+t}}=1.
\end{aligned}$$
□

定理 4.16 设 G 是有限正则 p-群, M,N 是 G 的正规子群. 则对任意的非负整数 s,t,i 有

(1) $[\mho_s(M),\mho_t(N)]=\mho_{s+t}([M,N])$;

(2) $[M,G]\le\Omega_s(G)$ 等价于 $[M,\mho_s(G)]=1$;

(3) $[\Omega_s(G),\mho_t(G)]\le\Omega_{s-t}(G)$, 这里对 $k\le 0$, 规定 $\Omega_k(G)=1$;

(4) $(\mho_s(G))_i=\mho_{si}(G_i)$;

(5) $G_{i+1}\le\Omega_s(G)$ 等价于 $\mho_s(G)\le Z_i(G)$.

证 (4) 可由 (1) 推出, (5) 可由 (2) 推出, 而 (1)–(3) 应用定理 4.15 立得. □

由这个定理可得到正则 p-群的幂结构与换位子结构之间的很多有趣的联系. 特别地, 由 (4), $\mho_1(G)$ 的幂零类 $\le e-1$, 其中 $e=e(G)$ 是 G 的幂指数. 又由 (3), 对任意的 s, 都有 $\Omega_s(G)$ 与 $\mho_s(G)$ 之间元素相乘可交换.

§5. 亚循环 p-群

本节在定义了亚循环 p-群并给出它的两个充分必要条件之后, 简单介绍一下最大类 p-群的知识, 最后给出奇阶亚循环 p-群的一个完全分类.

定义 5.1 称 p-群 G 为亚循环的，如果它有循环正规子群 $A = \langle a \rangle$，使商群 G/A 亦为循环群.

显然亚循环 p-群的子群和商群仍为亚循环的.

定理 5.2 (Blackburn) *有限 p-群 G 是亚循环群当且仅当 $G/\Phi(G')G_3$ 是亚循环的.*

证 显然只须证充分性，并可设 $\Phi(G')G_3 \neq 1$. 取 G 的 p 阶正规子群 $K \leq \Phi(G')G_3$，用归纳法可假定 G/K 是亚循环群，即存在 $L \trianglelefteq G$, $L \geq K$ 使 G/L 使 L/K 均为循环群. 若 L 循环，则 G 已为亚循环群. 故可设 L 非循环. 由 $K \leq Z(G)$，有 L 为交换群. 设 $L = M \times K$，令 $|M| = p^s$，必有 $s \geq 2$. 这因为 $1 < \Phi(G')G_3 < G' < L$，因此 $|L| \geq p^3$. 由 $\mho_1(M) = \mho_1(L)$，及 $L \trianglelefteq G$ 得 $\mho_1(M) \trianglelefteq G$. 令 $N = \mho_1(M)K$，我们有 $N \trianglelefteq G$，且 $|L : N| = p$. 于是又有 G/N 交换，(这因为 $L/N \leq Z(G/N)$ 及 G/L 循环)，从而 $G' \leq N$. 由

$$|G'/G' \cap \mho_1(M)| = |G'\mho_1(M)/\mho_1(M)| \leq |N/\mho_1(M)| = p,$$

得 $G' = G' \cap \mho_1(M)$ 或 $|G' : G' \cap \mho_1(M)| = p$. 若前者发生，必有 $K \leq G' \leq \mho_1(M) < M$，矛盾. 故有 $|G' : G' \cap \mho_1(M)| = p$. 因 $G' \cap \mho_1(M) \trianglelefteq G$，考虑 $\overline{G} = G/G' \cap \mho_1(M)$. 有 $|\overline{G}'| = p$. 于是 $\Phi(\overline{G}') = \bar{1}$, $\overline{G}_3 = 1$，故 $\Phi(G')G_3 \leq G' \cap \mho_1(M)$. 但 $K \leq \Phi(G')G_3$，故 $K \leq G' \cap \mho_1(M) < M$，矛盾. □

定理 5.3 *设 $p > 2$. 则有限 p-群 G 亚循环的充要条件为 $\omega(G) \leq 2$.*

证 必要性：设 G 亚循环，则 $G' \leq \mho_1(G)$，故

$$p^{\omega(G)} = |G/\mho_1(G)| = |G/\Phi(G)| \leq p^2,$$

于是 $\omega(G) \leq 2$.

充分性：由定理 5.2 可设 $\Phi(G')G_3 = 1$. 由 $\omega(G) \le 2$ 得

$$|G/\Phi(G)| \le |G/\mho_1(G)| \le p^2,$$

于是 $d(G) \le 2$. 除去循环群的情形，可设 $d(G) = 2$, 这时有 $\Phi(G) = \mho_1(G)$, 于是 $G' \le \mho_1(G)$. 令 $G = \langle a, b\rangle$, 有 $G' = \langle [a, b]\rangle$ 且 $|G'| \le p$. 这时可设 $[a,b] = x^{p^\alpha}$, $\alpha \ge 1$, 但 x 不是任一元的 p 次幂，即 $x \notin \mho_1(G) = \Phi(G)$. 由 Burnside 基定理，存在 $y \in G$ 使 $G = \langle x, y\rangle$. 因为 $G' \le \langle x\rangle \le G$, 而 $G/\langle x\rangle$ 循环，故 G 为亚循环. □

引理 5.4 设 P 是亚循环 p-群，p 是奇素数. 则

(1) P 是正则的；

(2) 若 $|P'| = p^n$, 则 P 是 p^n-交换的，即满足

$$(xy)^{p^n} = x^{p^n}y^{p^n},\ \forall x, y \in P;$$

(3) 若 $x, y \in P$ 且 m 是正整数，则

$$x^{p^m} = y^{p^m} \quad 当且仅当 \quad (x^{-1}y)^{p^m} = 1 \quad 当且仅当 \quad (xy^{-1})^{p^m} = 1;$$

(4) 若 $x, y \in P$ 且 m 是正整数，则

$$[x^{p^m}, y] = 1 \quad 当且仅当 \quad [x, y]^{p^m} = 1 \quad 当且仅当 \quad [x, y^{p^m}] = 1.$$

(证明从略.)

在给出亚循环 p-群的完全分类之前，简短介绍一下另一类重要的有限 p-群——最大类 p-群是适当的. 限于篇幅，我们不能给出这类有趣的 p-群的详尽的表述，有兴趣的读者可参看 B. Huppert 的 “Endliche Gruppen I” 第 III 章 §14.

定义 5.5 设 $n \ge 2$, 称 p^n 阶群 G 为最大类 p-群，如果 G 的幂零类 $c(G) = n - 1$.

最大类 p-群的简单性质是

命题 5.6 设 G 是 p^n 阶最大类 p-群. 则

(1) $G' = \Phi(G), |G/G'| = p^2, d(G) = 2$;

(2) $|G_i/G_{i+1}| = p, i = 2, 3, \cdots, n-1$;

(3) 对 $i \geq 2, G_i$ 是 G 中唯一的 p^{n-i} 阶正规子群;

(4) 若 $N \trianglelefteq G$, 且 $|G/N| \geq p^2$, 则 G/N 亦为最大类 p-群;

(5) 对于 $0 \leq i \leq n-1$ 有 $Z_i(G) = G_{n-i}$.

证 由 G 非循环, G/G' 亦非循环. 于是 $|G/G'| \geq p^2$. 又因 $c(G) = n-1$, 对 $i = 2, 3, \cdots, n-1$, 有 $|G_i/G_{i+1}| \geq p$. 于是必有 $|G/G'| = p^2$, $|G_i/G_{i+1}| = p$, 且 G/G' 为 p^2 阶初等交换群. 由此又得 $G' = \Phi(G)$ 且 $d(G) = 2$. (1), (2) 均得证.

(3) 设 N 是 G 的一个 p^{n-i} 阶的正规子群, 则 $c(G/N)$ 至多为 $i-1$. 于是 $(G/N)_i = G_iN/N = \bar{1}$, 即 $G_i \leq N$. 比较阶即得 $N = G_i$.

(4) 由 (3) 必有 $N = G_i$, 对某 $i \geq 2$. 于是 $G/N = G/G_i$ 亦为最大类 p-群.

(5) 由 $c(G) = n-1$ 有 $Z_{n-1}(G) = 1$. 由

$$1 = Z_0(G) < Z_1(G) < \cdots < Z_{n-2}(G) < Z_{n-1}(G) = G$$

且 $|G/Z_{n-2}(G)| \geq p^2$(若否, $G = Z_{n-2}(G)$, 矛盾), 得 $|Z_i(G)| = p^i$, $i \leq n-2$. 由 (3) 即得 $Z_i(G) = G_{n-i}$. □

最大类 2-群是很容易确定的.

定理 5.7 设 G 是 2^n 阶的最大类 2-群, 则 G 必同构于下列三种类型的群之一:

(I) 二面体群: $\langle a, b \mid a^{2^{n-1}} = b^2 = 1, b^{-1}ab = a^{-1}\rangle$, $n \geq 2$;

(II) 广义四元数群: $\langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, b^{-1}ab = a^{-1}\rangle$, $n \geq 3$;

(III) 半二面体群: $\langle a, b \mid a^{2^{n-1}} = b^2 = 1, b^{-1}ab = a^{-1+2^{n-2}}\rangle$, $n \geq 4$.

证 由命题 5.6, $d(G) = 2$, G/G' 是 4 阶初等交换 2-群. 若 $G' = 1$, 则 G 是 (I) 型群, 对应于 $n = 2$; 而若 $G' \neq 1$, 则有 G'/G_3

循环, 并因此 $|G'/\Phi(G')G_3| = 2$. 于是 $G/\Phi(G')G_3$ 是 8 阶非交换群, 即为二面体群或四元数群, 总之都是亚循环的. 由定理 5.2, G 亦亚循环. 于是有循环正规子群 $L \trianglelefteq G$ 使 G/L 循环. 因 $G' \le L$, 有

$$\exp(G/L) = |G/L| \le \exp(G/G') = 2,$$

即 L 是 G 的循环极大子群. 根据上册第 IV 章定理 5.14, G 只有四种互不同构的类型, 除去非最大类的一种, 即得 G 必同构于上述三种类型之一. 又易见上述三种群均为最大类 2-群, 定理得证. □

对于 $p > 2$ 的情形, 最大类 p-群的决定是十分困难的. 对于 $p = 3$, 我们已知最大类 3-群必为亚交换群, 且有一亚循环的极大子群. 对于亚交换的最大类 p-群的分类, 近年来已有一些结果. 但对于 $p > 3$, 还很少非亚交换的最大类 p-群分类方面的结果. 与此相关联的, 即使对 p^{p+1} 阶的非正则 p-群 (它们一定是最大类 p-群) 的分类至今尚未完成.

下面我们给出亚循环 p-群的一个完全分类, 它是 M.F. Newman 和本书作者在 1987 年得到的. 有趣的是, 从六十年代末开始, 已有不少人给出了亚循环 p-群的分类, 但截止到 1987 年底, 已经发表的对于亚循环 2-群的分类还没有一个是完全正确的.

下面我们先给出亚循环 p-群的一个例子.

例 5.8 设 p 为奇素数, r, s, t, u 为非负整数, 且满足 $r \ge 1, u \le r$. 则

$$\langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, b^{-1}ab = a^{1+p^r} \rangle \tag{5.1}$$

是亚循环群, 且对于参数 r, s, t, u 的不同取值, 对应的亚循环群互不同构. 我们用 $< r, s, t, u; p >$ 来记这个群. 又, $< r, s, t, u; p >$ 是可裂的, 即可表成循环群被循环群的可裂扩张的充要条件为 $stu = 0$.

证　由 III, 3.11, (5.1) 式确实给出一个 p^{r+s+u} 阶的循环群被 p^{r+s+t} 阶循环群的扩张. 令这个群为 P, 则易验证下述事实:

(i) $|P| = p^{2r+2s+t+u}$;

(ii) $\exp P = p^{r+s+t+u} = o(b)$;

(iii) $P' = \langle a^{p^r} \rangle$, $|P'| = p^{s+u}$, 且

$$\overline{P} = P/P' = \langle \bar{a}, \bar{b} \mid \bar{a}^{p^r} = 1,\ \bar{b}^{p^{r+s+t}} = 1,\ \bar{a}^{\bar{b}} = \bar{a} \rangle;$$

(iv) $Z(P) = \langle a^{p^{s+u}} \rangle \langle b^{p^{s+u}} \rangle$.

由 (iii), r, $s+u$ 和 $r+s+t$ 是 P 的不变量; 而由 (ii), $r+s+t+u$ 也是不变量, 于是 r, s, t 和 u 都是 P 的不变量. 因此, 参数 r, s, t, u 的不同取值对应于不同构的亚循环群.

下面证明 P 可裂的充分必要条件是 $stu \neq 0$. 首先, 如果 $s=0$, 则 $\langle b \rangle \geq \langle a^{p^r} \rangle$, 因此 $\langle b \rangle \trianglelefteq P = \langle b, ab^{-p^t} \rangle$. 因为 $(ab^{-p^t})^{p^r} = a^{p^r} b^{-p^{r+t}} = 1$, 我们有 $\langle b \rangle \cap \langle ab^{-p^t} \rangle = 1$, 于是 P 是可裂的. (注意 P 是 p^{s+u}-交换的, 因此也是 p^r-交换的.) 如果 $t=0$, 我们有 $(ba^{-1})^{p^{r+s}} = 1$, $P = \langle a, ba^{-1} \rangle$, 于是 $\langle a \rangle \cap \langle ba^{-1} \rangle = 1$. P 也可裂. 而如果 $u=0$, P 显然是可裂的.

反过来, 假定 $stu \neq 0$, 我们将证明 P 不是可裂的. 若 P 可裂且 $P = \langle x \rangle \langle y \rangle$, $\langle x \rangle \cap \langle y \rangle = 1$, $\langle x \rangle \trianglelefteq P$. 因为 $\exp P = \max(o(x), o(y))$, 我们有 $(o(x), o(y)) = (p^{r+s+t+u}, p^{r+s})$ 或 $(p^{r+s}, p^{r+s+t+u})$. 又因 $|P'| = p^{s+u}$, $P' \leq \langle x \rangle$, P/P' 应有不变量 (p^{r+t}, p^{r+s}) 或 $(p^{r-u}, p^{r+s+t+u})$; 另一方面, P/P' 应有不变量 (p^r, p^{r+s+t}), 这与 $stu \neq 0$ 矛盾. □

在证明定理 5.10 之前, 我们不加证明地叙述下面的引理.

引理 5.9 设 p 是奇素数, n 是正整数. 假定 $U = U(p^n)$ 是由 $\mathbb{Z}/p^n\mathbb{Z}$ 的可逆元组成的乘法群, 即

$$U = \{x \in \mathbb{Z}/p^n\mathbb{Z} \mid (x, p) = 1\}.$$

设 $S(U) \in \mathrm{Syl}_p(U)$. 则

$$S(U) = \{x \in U \mid x \equiv 1 (\mathrm{mod}\ p)\},$$

并且 $S(U)$ 是 p^{n-1} 阶循环的. $S(U)$ 的唯一的 p^i 阶子群 $S_i(U)$, $0 \leq i < n$, 是

$$S_i(U) = \{x \in U \mid x \equiv 1 (\mathrm{mod}\ p^{n-i})\}.$$

定理 5.10 设 p 是奇素数，P 是亚循环 p-群. 则 P 同构于例 5.8 中的一个群.

证　首先，由 III,3.11, P 有下列定义关系：

$$P = \langle x, y \mid x^{p^n} = 1,\ y^{p^m} = x^{p^k},\ x^y = x^{1+ip^l} \rangle \tag{5.2}$$

其中 n, m, k, l, i 是正整数，$k \le n, l \le n, p\nmid i, k+l \ge n$ 并且 $(1+ip^l)^{p^m} \equiv 1 (\mathrm{mod}\ p^n)$. 由引理 5.9, 我们有 $l+m \ge n$ 并且存在整数 j 使 $(1+ip^l)^j \equiv 1+p^l (\mathrm{mod}\ p^n)$. 用 $x' = x^j$ 和 $y' = y^j$ 代替 x 和 y, 我们有

$$P = \langle x', y' \mid x'^{p^n} = 1,\ y'^{p^m} = x'^{p^k},\ x'^{y'} = x'^{1+p^l} \rangle. \tag{5.3}$$

其中 n, m, k, l 是正整数并满足 $n \ge k, n \ge l, n-l \le m$ 和 $n-l \le k$. 因为 $P' = \langle x'^{p^l} \rangle$, 由引理 5.4(2), P 是 p^{n-l}-交换的. 下面我们将反复应用这个事实.

若 $m \ge k \ge l$, (5.3) 式就是我们需要的定义关系. 如若不然，我们将有下面两种可能性：

情形 1　$m < k$.

先设 $l \le m$. 令 $a = x'$, $b = x'^{1-p^{k-m}}y'$, 因为 $n-l \le m$, 我们有

$$\begin{aligned}
a^{p^n} &= 1, \\
b^{p^m} &= (x'^{1-p^{k-m}}y')^{p^m} = x'^{p^m - p^k} y'^{p^m} = x'^{p^m} = a^{p^m}, \\
a^b &= x'^{x'^{1-p^{k-m}}y'} = x'^{y'} = x'^{1+p^l} = a^{1+p^l}.
\end{aligned}$$

这时 P 有所需的定义关系

$$P = \langle a, b \mid a^{p^n} = 1,\ b^{p^m} = a^{p^m}, a^b = a^{1+p^l} \rangle.$$

再设 $l > m$. 令 $x'' = y'x'^{p^{l-m} - p^{k-m}}$, $y'' = x'$, 我们有

$$x''^{p^m} = (y'x'^{p^{l-m} - p^{k-m}})^{p^m} = y'^{p^m} x'^{p^l - p^k} = x'^{p^l},$$

于是 $\langle x''\rangle \geq \langle x'^{p^l}\rangle = P'$, 因而有 $\langle x''\rangle \trianglelefteq P$. 因 $o(x'^{p^l}) = p^{n-l}$, 有 $o(x'') = p^{n+m-l}$. 又有

$$\begin{aligned}
y''^{p^l} &= x'^{p^l} = x''^{p^m},\\
x''^{y''} &= (y'x'^{p^{l-m}-p^{k-m}})^{x'} = y'^{x'}x'^{p^{l-m}-p^{k-m}}\\
&= y'(y'^{-1}x'y')^{-1}x'^{1+p^{l-m}-p^{k-m}} = y'x'^{-1-p^l+1+p^{l-m}-p^{k-m}}\\
&= (y'x'^{p^{l-m}-p^{k-m}})x'^{-p^l} = x''^{1-p^m}.
\end{aligned}$$

和前面一样, 存在整数 i 使 $(1-p^m)^i \equiv 1+p^m \pmod{p^n}$. 令 $a = x''^i, b = y''^i$, 我们得到所需的定义关系

$$P = \langle a, b \mid a^{p^{n+m-l}} = 1,\ b^{p^l} = a^{p^m},\ a^b = a^{1+p^m}\rangle.$$

情形 2 $m \geq k$ 和 $l > k$.

这时有 $\langle y'\rangle \geq P'$, 因而 $\langle y'\rangle \trianglelefteq P$.

令 $x'' = y'$, $y'' = y'^{-p^{m-k}}x'$, 我们有

$$\begin{aligned}
x''^{p^{n+m-k}} &= 1,\\
y''^{p^k} &= (y'^{-p^{m-k}}x')^{p^k} = y'^{-p^m}x'^{p^k} = 1 = x''^{p^{n+m-k}},\\
x''^{y''} &= y'^{x'} = y'(y'^{-1}x'y')^{-1}x' = y'x'^{-p^l} = y'(x'^{p^k})^{-p^{l-k}}\\
&= y'^{1-p^{m+l-k}} = x''^{1-p^{m+l-k}}.
\end{aligned}$$

因为 $k < n+m-k$, 我们已把这种情形归结到情形 1. 这样在任何情形下我们都得到所需的定义关系.

最后, 若 P 由 (5.1) 式给出, 则我们有 $[a^{p^{r+s}}, b] = 1$. 据引理 5.4(4), 我们有 $1 = [a,b]^{p^{r+s}} = a^{p^{2r+s}}$, 因此 $2r+s \geq r+s+u$, $u \leq r$. 定理证毕. □

注 5.11 如果 $p=2$, 除了在 IV, 定理 5.14 中决定的具有循环极大子群的有限 2-群当然都是亚循环 2-群外, 只有下面的两种彼此互不同构的亚循环 2-群:

(I) 通常的亚循环 2-群:

$$P = \langle a, b \mid a^{2^{r+s+u}} = 1,\ b^{2^{r+s+t}} = a^{2^{r+s}}, a^b = a^{1+2^r}\rangle,$$

其中 r, s, t, u 是非负整数满足 $r \geq 2$ 和 $u \leq r$.

这类群很类似例 5.8 中定义的奇阶亚循环 p-群，我们也有 P 可裂的充分必要条件是 $stu = 0$.

(II) 特殊亚循环 2-群:

(II-1) 可裂的特殊亚循环 2-群: $P = \langle a, b \mid a^{2^{r+s+v+t'}} = 1,\ b^{2^{r+s+t}} = 1, a^b = a^{-1+2^{r+v}} \rangle$ 其中 r, s, v, t, t' 是非负整数满足 $r \geq 2$, $t' \leq r$, $tt' = sv = tv = 0$.

(II-2) 不可裂的特殊亚循环 2-群: $P = \langle a, b \mid a^{2^{r+s+v+t'-1}} = 1,\ b^{2^{r+s+t}} = a^{2^{r+s+v+t'}}, a^b = a^{-1+2^{r+v}} \rangle$ 其中 r, s, v, t, t' 是非负整数满足 $r \geq 2$, $t' \leq r - 2$, $u \leq 1$, $tt' = sv = tv = 0$.

上述不同类型的群或者同一类型但具有不同的参数值的群彼此互不同构. 并且它们和定理 IV,5.14 中决定的群也互不同构.

我们略去这个结果的颇为冗长的证明，感兴趣的读者可参看下列未公开发表的文章 (可向作者索要复印件):

M.F. Newman and Ming-Yao Xu (徐明曜), *A classification of metacyclic p-groups,* Research Report No. 32/1990, Institute of Mathematics and Department of Mathematics, Peking University; 19 pages.

习 题

1. 设 G 是有限 p-群, $e(G) > 0$. 证明 G 的下幂群列任二项间都是真包含关系，即 $\mho_i(G) > \mho_{i+1}(G)$ $i = 0, 1, \cdots, e-1$.

2. 举例说明对任意的 $e > 0$, 存在有限 p-群 G 使 $e(G) = e$, 并且

$$1 = \Omega_0(G) < \Omega_1(G) = \Omega_2(G) = \cdots = \Omega_e(G) = G.$$

3. 证明对称群 S_{p^2} 的 Sylow p-子群 $Z_p \wr Z_p$ 是 p^{p+1} 阶非正则群，其幂零类为 p.

4. 设 G 是由下述定义关系确定之 3^5 阶群: $G = \langle a, b \rangle$, $a^{3^3} = b^{3^2} = 1$, $a^b = a^4$. 则 G 是正则 3-群. 但 $G \times G$ 是非正则群. 由此可见正则群的直积不一定正则.

5. 设 G 是正则 3-群, $d(G) = 2$. 则对 $s \geq 3$, 有 $G_s \leq \mho_{s-2}(G')$.

6. 设 G 是群，满足 $[g,h,h]=1$, $\forall g,h\in G$. 则 G 是幂零群，且 $c(G)\leq 3$. 又若 G 中没有 3 阶元素，则 $c(G)<3$.

7. 设 G 是群，满足 $\exp(G)=3$. 又设 G 可由 d 个元素生成，则 $|G|\leq 3^n$, 其中 $n=d+\binom{d}{2}+\binom{d}{3}$.

8. 设 G 是极小非正则 p-群，且 $c(G)=c$, $\exp(G)=p^e$. 则成立下列事实：

(1) G 可由两个元素 a,b 生成，且满足 $(ab)^p=a^pb^p$.

(2) 若 $e>2$, 则对所有的 s, $1\leq s\leq e$, 有 $\Omega_s(G)=\Lambda_s(G)$, $\mho_s(G)=V_s(G)$, 和 $G/\Omega_s(G)\cong\mho_s(G)$.

(3) 令 $M(G)=\langle u \mid (au)^p=a^p,\ \forall a\in G\rangle$. 则 $M(G)=G'$.

9. 如果有限 p-群 G 没有方次数为 p 且阶大于 p^{p-2} 的正规子群，则 G 是正则 p-群.

10. 设有限 p-群 G 有一个交换极大子群. 则 G 正则当且仅当 $c(G)<p$.

11. 设 G 是有限 p-群. 如果 $Z(G)$ 包含 p^2 阶的初等交换子群 N, 使得对任意的 p 阶子群 $M\leq N$, G/M 都是正则的，则 G 也正则.

12. 称有限 p-群 G 内正则，如果 G 非正则，但它的每个真子群均正则. 假定 G 是内正则 p-群且 $c(G)=c$, $\exp(G')=p$. 则成立下列事实：

(1) G 可由二元生成.

(2) $(x[y,z])^p=x^p$ 且 $[x^p,z]=1$, $\forall x,y,z\in G$.

(3) $\mho_1(G)\leq Z(G)\leq\Phi(G)$; $Z_{c-1}(G)=\Phi(G)$.

(4) G 的每个真子群的幂零类小于 c.

(5) G 是 p^2-交换的.

13. 假定有限 p-群 G 有一正规子群 N. 称 N正则嵌入于G, 如果对于任意的 $a\in G$, $b\in N$, 均有

$$(ab)^p=a^pb^pc_3^p\cdots c_m^p,$$

其中 $c_i\in\langle a,b\rangle'$.

设 $N\lhd G$. 证明若 $|N|\leq p^{p-1}$ 或 $N\leq Z_{p-1}(G)$, 则 N 正则嵌入于 G.

14. 设 $N\lhd G$. 证明 N 正则嵌入于 G 当且仅当对任意的 $a\in G$, $\langle a,N\rangle$ 是正则的.

15. 称有限 p-群 N 为完全正则的，如果只要有 $N\lhd G$, G 是另一个有限 p-群，则 N 就正则嵌入于 G.

证明交换 p-群 N 是完全正则的，当且仅当 $|N:\mho_1(N)|\leq p^{p-2}$ 或 $|N|=p^{p-1}$.

16. 设 N 是 3-群. 若 N 的每个截断都是完全正则的，则 N 是循环群或 9 阶初等交换群.

17. 称有限 p-群 G 为 p^s-Φ-正则的，如果对任意的 $a,b\in G$,

$$(ab)^{p^s}=a^{p^s}b^{p^s}c_3^{p^s}\cdots c_m^{p^s},$$

其中 $c_i \in \Phi(\langle a,b\rangle)$.

证明若 G 是 p^s-Φ-正则的，则成立下列事项：

(1) $\Omega_s(G) = \Lambda_s(S)$.

(2) $\mho_s(G) = V_s(G)$.

(3) 对任意的 $a,b \in G$, 如果 $a^{p^s} = b^{p^s}$, 则有整数 $n \equiv 1 \pmod p$ 使得 $(ab^{-n})^{p^s} = 1$.

(4) 对任意的 $a,b \in G$, 如果 $(ab^{-1})^{p^s} = 1$, 则有整数 $m \equiv 1 \pmod p$ 使得 $a^{p^s} = b^{mp^s}$.

(5) $|G/\Omega_s(G)| = |\mho_s(G)|$.

18. 构造有限 p-群，使得它是 p^s-Φ-正则的，但不是 p^s-正则的.

19. 称有限 p-群 G 为 Φ-正则的, 如果对任意的 $a,b \in G$,

$$(ab)^p = a^p b^p c_3^p \cdots c_m^p,$$

其中 $c_i \in \Phi(\langle a,b\rangle)$.

证明若 G 是 Φ-正则的，则对任意的 s, G 也是 p^s-Φ-正则的.

20. 决定极小非亚循环 p-群. (一个群称为极小非亚循环群，如果它不是亚循环群，但它的每个真截断都是亚循环的.)

21. 设 G 是正则 p-群， $\mho_1(G') = 1$, $r(G) = r$, 其中 $r(G)$ 是 G 的导列长. 则 $c(G) \le \frac{1}{2}(2p-1)^{r-1} + \frac{1}{2}$.

第 XI 章

典型群

域 $\mathbf{F}$ 上向量空间 V 上全体可逆线性变换对于线性变换乘法构成一个群，叫做 V 上 *一般线性群*, 记作 $GL(V)$. $GL(V)$ 中满足某些给定条件 ——例如对应的矩阵行列式为 1 或保持 V 上某个"型"不变 ——的元素集合构成了 *典型群*, 具体地说，典型群或者是 *线性群* 或者是作用在定义了型的空间，即 *度量空间* 上的可逆线性变换群，其中包括 *辛群*, *酉群* 和 *正交群* 及由上述各类群所导出的射影空间上的 *共线变换群*. 典型群是极为重要的一个群类，是我们在本书中所考虑的两个具体群类之一. 有限群论的各个领域，都要用到关于典型群的结果. 通过对典型群结构的讨论，我们可以更好地掌握一般的群论研究方法. 此外，通过由度量空间所导出的 *射影空间*, 我们可以得到一系列的几何 (或者说组合) 结构，例如 Tits *几何*, *配极几何*, *设计* 等等. 这些几何，都是当前一些十分重要并且活跃的领域.

典型群的理论内容十分丰富，我们只能介绍有限域上度量空间和典型群的基本理论和方法. 由于域上向量空间 V 上典型群中元素均为 V 的可逆线性变换，因此在讨论过程中，我们将直接引用线性代数的一些结论.

本章的编排如下： §1 介绍线性群的定义和最基本的性质； §2 度量空间和典型群基本理论初步； §3 介绍射影空间理论； §4 讨论 $PSL(2,q)$ 的结构和性质.

§1. 一般线性群简介

本节考察一般线性群，主要介绍有关线性群的基本概念和性质.

定义 1.1 设 V 为 $\mathbf{F}$ 上 n 维向量空间， $GL(V)$ 表示 V 上全体可逆线性变换之集合，它在映射乘法之下组成一个群，叫做 V 上 **一般线性群**. 又 $\mathbf{F}$ 上全体非奇异 $n\times n$ 矩阵对于矩阵乘法也构成一个群，记作 $GL(n,\mathbf{F})$. 令 $\alpha\in GL(V)$, $\mathrm{Mat}(\alpha)$ 为 α 在 V 上给定的基下的矩阵， 映射 $\tau: g\mapsto \mathrm{Mat}(g)$ 确定了一个由 $GL(V)$ 到 $GL(n,\mathbf{F})$ 的同构对应. 以 $SL(V)$ 表示 V 上全体对应矩阵的行列式为 1 的线性变换所组成的集合， $SL(V)$ 叫做 V 上 **特殊线性群**, $SL(V)$ 在上述映射下的像记作 $SL(n,\mathbf{F})$. $GL(n,\mathbf{F})$ 和 $SL(n,\mathbf{F})$ 分别叫做 $\mathbf{F}$ 上 n 级 **一般线性群** 和 n 级 **特殊线性群**. 我们通过映射 $\varphi: M\mapsto \det M$ 把 $GL(V)$ 映到 $\mathbf{F}^{\#}$ 上，这是一个同态对应，且 $\mathrm{Ker}\ \varphi = SL(V)$, 因此 $SL(V)\trianglelefteq GL(V)$. 若 $\mathbf{F}=GF(q)$, 则 $GL(n,\mathbf{F})$ 和 $SL(n,\mathbf{F})$ 分别记作 $GL(n,q)$ 和 $SL(n,q)$.

设 V 为 $\mathbf{F}$ 上 n 维向量空间， $\{v_1,v_2,\cdots,v_n\}$ 为 V 中一组固定基，则 V 中任意向量 v 均可表为以下形状： $v=\sum\limits_{i=1}^{n} x_iv_i, x_i\in\mathbf{F}$. 我们把 n-元组 $(x_1,x_2,\cdots,x_n)$ 称为 v 在基 $\{v_1,v_2,\cdots,v_n\}$ 之下的坐标，记作 X_v. 显然 V 中每个向量由它的坐标唯一确定. 设 $g\in GL(V)$, 则有 $X_{v^g}=X_v\mathrm{Mat}(g)$.

在本节中，除非特别声明，总假定 $\mathbf{F}=GF(q)$, q 为素数幂; V 表示 $\mathbf{F}$ 上 n 维向量空间; 所有矩阵均指 $\mathbf{F}$ 上 n 级矩阵.

在此我们还固定两个在本章中常用的符号：若 $\mathbf{F}$ 为一域，记 $\mathbf{F}^{\#}=\mathbf{F}\backslash\{0\}$; 若 G 为一群，令 $G^{\#}=G\backslash\{1\}$.

以 $\mathbf{I}$ 表示 n 级单位矩阵， $\mathbf{E}_{ij}$ 表示 (i,j)-元为 1 其它元为零的 $n\times n$ 矩阵. 设 $\lambda,\delta\in\mathbf{F}$, $\delta\neq 0$, 令 $\mathbf{B}_{ij}(\lambda)=\mathbf{I}+\lambda\mathbf{E}_{ij}$, $i\neq j$, $\mathbf{D}_\delta$ 表示对角矩阵 $\mathrm{diag}\{1,1,\cdots,1,\delta\}$. 注意， $\mathbf{B}_{ij}(\lambda)^{-1}=\mathbf{B}_{ij}(-\lambda)$.

通过矩阵计算可得如下的：

命题 1.2 $SL(n,\mathbf{F}) = \langle \mathbf{B}_{ij}(\lambda) \mid i \neq j, \lambda \in \mathbf{F}\rangle$, $GL(n,\mathbf{F}) = \langle \mathbf{B}_{ij}(\lambda), \mathbf{D}_\delta \mid i \neq j, \lambda \in \mathbf{F}, \delta \in \mathbf{F}^{\#}\rangle$.

下面讨论 $GL(V)$ 和 $SL(V)$ 的性质. 首先我们引入一些符号: 对于任意的 $v \in V$, $g \in GL(V)$, 我们以 $\langle v\rangle$ 或 $\mathbf{F}v$ 表示由 v 生成的一维子空间; 记 $[v,g] = -v + v^g$, $[V,g] = \langle [u,g] \mid u \in V\rangle$, $C_V(g) = \{u \in V \mid u^g = u\}$; $\mathrm{Stab}\ v = \{h \in GL(V) \mid v^h = v\}$.

设 V 为 n 维向量空间, $\{v_i \mid 1 \leq i \leq n\}$ 为 V 的一组固定的基. V 中一个 $(n-1)$-维子空间 W 说是 V 的一个*超平面*. $GL(V)$ 中一个元素 s 叫做一个*平延*, 若 $s \neq 1$, s 固定超平面 W 中每个向量, 且 $U = [V,s] \subseteq W$. 显然有 $\dim U = 1$, 即 $\exists u \in V$, 使 $U = \langle u\rangle$. 这时 W 说是平延 s 的*轴*. U 说是平延 s 的*中心*.

命题 1.3 (1) $s \in GL(V)$ 为平延当且仅当在适当的基下, $\mathrm{Mat}(s) = \mathbf{B}_{ij}(\lambda), i \neq j, \lambda \in \mathbf{F}^{\#}$.

(2) 设 $\dim V > 1$, u 为 V 中非零向量, 则 Stab u 中有交换子群 R, 使 $R \trianglelefteq \mathrm{Stab}\ u$, 且 $SL(V) = \langle R^g \mid g \in SL(V)\rangle$.

证 (1) 设 $\{v_i \mid 1 \leq i \leq n\}$ 为 V 的一组基, t 为 V 上一个线性变换, 且 t 在所给基之下的矩阵为 $\mathbf{B}_{ij}(\lambda)$, $\lambda \in \mathbf{F}^{\#}$. 显然 t 为以 $\langle v_1, \cdots, v_{i-1}, v_{i+1}, \cdots, v_n\rangle$ 为轴, $\langle v_i^t - v_i\rangle$ 为中心的平延.

反之, 令 t 为一平延. 由定义, t 固定一个超平面 W 中所有的元. 又有 $u \in V$ 能使 $u^t \neq u$, 且 $u^t - u \in W$. 记 $v_2 = u$, 选择 W 的一组基: $v_1 = u^t - u, v_2, v_3, \cdots, v_n$, 显然 $\{v_i \mid 1 \leq i \leq n\}$ 为 V 的一组基, 且在这一组基下, t 的对应矩阵为 $\mathbf{B}_{12}(1)$.

(2) 设 $\{v_i \mid 1 \leq i \leq n\}$ 为 V 的一组基, 其中 $v_1 = u$. 令 $R = \langle s_i \mid \mathrm{Mat}(s_i) = \mathbf{B}_{i1}(\lambda), \lambda \in \mathbf{F}^{\#}, 2 \leq i \leq n\rangle$. 简单计算表明, R 为可换群, 且 $R \trianglelefteq \mathrm{Stab}\ u$, $SL(V) = \langle R^g \mid g \in SL(V)\rangle$. □

定理 1.4 令 V 为域 $\mathbf{F}$ 上 n 维向量空间, 记 $G = GL(V)$, $L = SL(V)$. 则

(1) G 中的所有平延均包含在 L 中, 且 L 由平延生成.

(2) G 中的所有平延构成一个共轭类, 且当 $n \geq 3$ 时所有平延在 L 中互相共轭,

(3) $G' = L' = L$, 除非 $n = 2$, $|\mathbf{F}| \leq 3$.

证 (1) 是显然的.

(2) 由命题 1.3(1) 的证明过程可知, 任意两个平延在 G 中互相共轭. 且若 $t \in L$ 为以 W 为轴, U 为中心的平延, 则对任意的 $x \in G$, t^x 为以 W^x 为轴 U^x 为中心的平延. 现在证明 (2) 的后一部分. 设 f, g 均为平延, 则有 $x \in G$ 能使 $f = x^{-1}gx$. 选择 V 的基 $\{v_i \mid 1 \leq i \leq n\}$, 使得 $\mathrm{Mat}(f) = \mathbf{B}_{12}(1)$. 令 $\delta = \det x$, 取 $y \in G$, 使 $\mathrm{Mat}(y) = \mathbf{D}_\delta$, 由于 $n \geq 3$, 故 y 固定 v_1 及 v_2, 从而有 $y^{-1}fy = f = x^{-1}gx$. 令 $z = xy^{-1}$, 则 $f = z^{-1}gz$, 且显然 $z \in L$.

(3) 我们证明, 任意平延都可表为换位子, 除非 $n = 2$, $|\mathbf{F}| \leq 3$. 令 $\{v_1, v_2, \cdots, v_n\}$ 为 V 的一组基. 令 $W = \langle v_1, \cdots, v_{n-1}\rangle$, s, t 均为 W 上平延且使 $v_n^s = v_n + v_2$, $v_n^t = v_n + v_1$, 则 st 也为平延. 故由 (2), 有 $h \in SL(V)$ 能使 $st = s^h$, 从而 $t = s^{-1}(st) = s^{-1}s^h$ 为一个换位子. 现假定 $n = 2$, $|\mathbf{F}| > 3$. 令 $t(b) = \mathbf{B}_{21}(b)$, $g = \mathrm{diag}\{a, a^{-1}\}$. 则 $t(b)^g = t(a^2b)$, 由假定 $|\mathbf{F}| > 3$, 故可选择 a 使 $a^2 \neq 1$, 则 $t(b) = [t((a^2-1)^{-1}b), g]$, 即 $t(b)$ 为一个换位子. □

命题 1.5 *$C_{GL(V)}(SL(V)) = Z(GL(V)) \cong \mathbf{F}^{\#}$. 特别地, $Z(SL(V))$ 同构于由 $\mathbf{F}^{\#}$ 中满足条件 $a^n = 1$ 的元 a 所组成的循环群.*

证 设 $z \in C_{GL(V)}(SL(V))$, 则 z 与 $GL(V)$ 中一切平延可换, 故 $\mathrm{Mat}(z)$ 与一切 $\mathbf{B}_{ij}(\lambda)$ 可换, 从而 $\mathrm{Mat}(z)$ 为数量矩阵, 即 z 为数量变换, 从而 $z \in Z(GL(V))$. 又由以上讨论易知 $z = a1_V \mapsto a$, $a \in \mathbf{F}^{\#}$ 为 $Z(GL(V))$ 到 $\mathbf{F}^{\#}$ 的同构对应. 最后的结论是显然的.
□

命题 1.6 *设 $\mathbf{F}$ 为特征 p 的有限域, $|\mathbf{F}| = q = p^m$, 则*

(1) $|GL(n,q)| = q^{n(n-1)/2}\prod\limits_{i=1}^{n}(q^i - 1)$;

(2) $|SL(n,q)| = |GL(n,q)|/(q-1)$.

证 (1) 和 (2) 即第 I 章命题 3.17(1), (2). □

定理 1.7 设 V 为 $\mathbf{F}=GF(q)$ 上 n 维向量空间，记 $G=GL(n,q)$, $L=SL(n,q)$. 令 G 和 L 分别等同于 $GL(V)$ 和 $SL(V)$.

$$令U=\left\{\left(\begin{array}{cccc}1&\alpha&\beta&\cdots\\&1&&\\&&\ddots&\\0&&&1\end{array}\right)\middle|\alpha,\beta,\cdots\in\mathbf{F}\right\},$$

$$D=\{\mathrm{diag}\{a_1,a_2,\cdots,a_n\}\mid a_i\in\mathbf{F}^{\#}\}.$$

则成立

(1) $U\in\mathrm{Syl}_p(G)$;

(2) D 为 G 的子群，且 $|D|=(q-1)^n$, 又 $N_G(U)=DU$;

(3) 若 $q>2$, 则 $C_G(D)=D$;

(4) $N_G(D)/D\cong S_n$;

(5) $|D\cap L|=(q-1)^{n-1}$, 且成立 $N_L(D\cap L)=N_G(D)\cap L$, 除非 $n=2$, $|\mathbf{F}|\le 3$.

证 (1) 和 (2) 均可通过简单矩阵计算得出.

(3) 显然 D 为可换群. 若 $q>2$, 把 D 看作是 V 上线性变换群，则 $\mathbf{F}v_i$, $1\le i\le n$, 是 V 中全部在 D 作用下不变的一维子空间. $\forall c\in C_G(D)$, $d\in D$ 成立: $(v_i^c)^d=(v_i^d)^c=(a_iv_i)^c=a_i(v_i^c)$. 故 v_i^c 属于某一 $\mathbf{F}v_{i'}$, 即有某个 i', 使 $v_i^c=b_iv_{i'}$, $b_i\in\mathbf{F}^{\#}$. 我们证明 $i=i'$, $\forall i\in\{1,2,\cdots,n\}$. 假定有 i, $i\ne i'$, 使对某个 $b\in\mathbf{F}^{\#}$ 有 $v_i^c=bv_{i'}$. 取 $d\in D$, $d=\mathrm{diag}\{a_1,\cdots,a_i,\cdots,a_{i'},\cdots,a_n\}$, 其中 $a_i=1$, $a_{i'}\ne 1$. $bv_{i'}=v_i^c=(v_i^d)^c=(v_i^c)^d=(bv_{i'})^d=a_{i'}(bv_{i'})$, 矛盾.

(4) 对任意的 $d\in D$ 及 $g\in N_G(D)$, 有 $b_i\in\mathbf{F}^{\#}$, 能使 $(v_i^g)^d=v_i^{(gdg^{-1})g}=b_i(v_i^g)$, 故 $\langle v_i^g\rangle$ 在 D 作用下不变，从而 $v_i^g=b_iv_{i'}$. 反之，若 $v_i^g=b_iv_{i'}$, $\forall i\in\{1,2,\cdots,n\}$, 则显然成立 $g\in N_G(D)$, 记 $\Omega=\{\langle v_i\rangle\mid 1\le i\le n\}$. 则由以上讨论， $N_G(D)$ 作用在 Ω 上，作用核为 D, 且 $N_G(D)$ 在 Ω 上的作用导出 Ω 上的全体置换，特别地，我们有 $N_G(D)/D\cong S_n$. 这就证明了 (4).

(5) 我们仅需证明，若 $\dim V \geq 3$ 或 $n=2, q>3$, 则 $\langle v_i \rangle$ 为 V 中仅有的在 $D \cap L$ 作用下不变的一维子空间；因若上述结论成立，则 $N_G(D\cap L)=N_G(D)$, 且从而有 $N_L(D\cap L)=N_G(D)\cap L$. 设 $\langle v\rangle$ 在 $D\cap L$ 作用下不变， $v=\sum\limits_{i=1}^{n} b_i v_i$, 其中 $b_1 \neq 0$. 今证明 $v=b_1v_1$. 设 $d\in L$ 能使 $v_1^d=av_1$, $v_2^d=a^{-1}v_2$, $v_i^d=v_i$, $i\geq 3$, 其中 $1\neq a\in \mathbf{F}^{\#}$. 若 $q>3$, 可假定 $a^2\neq 1$, 则有 $e\in \mathbf{F}^{\#}$, 能使 $ev=v^d=ab_1v_1+a^{-1}b_2v_2+\sum_{i=3}^{n} b_iv_i$, 故有 $a=e$, 且 $b_i=0, \forall i\geq 3$. 交换 v_2 和 v_3 的位置，则可知 $b_2=0$. 故当 $n\geq 3$ 时结论成立. 若 $n=2, q>3$, 则 $ab_2=eb_2=a^{-1}b_2$. 因 $a^2\neq 1$, 便有 $b_2=0$. 这就证明了 $n=2$ 时结论也成立. □

§2. 典型群

本节中，我们考察有限域上度量空间及与之相关的典型群.

欧氏空间是实数域上的度量空间，有限域上度量空间和欧氏空间的理论是一脉相承的. 度量空间一个重要性质是, 在其中 Witt 引理成立：若 X 与 Y 都是度量空间 V 的子空间，且 φ 为 X 到 Y 的等距, 即保型同构, 则 φ 可扩充为度量空间 V 的自同构. 利用这一性质，我们可以得到相应度量空间的结构，对它们加以分类；并且在此基础上，讨论各种典型群的结构和基本性质.

假定 $\mathbf{F}$ 为有限域； V 为 $\mathbf{F}$ 上有限维向量空间. 读者会注意到，许多讨论同样适用于一般域上有限维向量空间的情况.

定义 2.1 设 V 为 $\mathbf{F}$ 上 n 维向量空间， $f: V\times V\to \mathbf{F}$ 说是 V 上数量积. 且

(1) f 说是**双线性的**, 若 $\forall u,v,w\in V$, $a\in \mathbf{F}$, $f(au,v)=f(u,av)=af(u,v)$; $f(u+w,v)=f(u,v)+f(w,v)$, $f(u,v+w)=f(u,v)+f(u,w)$.

(2) f 说是**斜对称的**, 若 f 是双线性的，且 $\forall u\in V$ 成立 $f(u,u)=0$. (注意：若 $\operatorname{char} \mathbf{F}\neq 2$, $f(u,u)=0, \forall u\in V$ 等价于条件 $f(u,v)=-f(v,u), \forall u,v\in V$)

(3) f 说是 对称的, 若 f 是双线性的, 且 $\forall u,v\in V$ 成立 $f(u,v)=f(v,u)$.

如下定义的映射 $Q:V\to\mathbf{F}$ 说是 V 上与 f 相连带的 二次型, 若 $\forall u,v\in V$, 成立:

(i) $Q(au)=a^2Q(u)$, $\forall a\in\mathbf{F}$.

(ii) $Q(u+v)=Q(u)+Q(v)+cf(u,v)$, 其中 $c=2$, 若 char $\mathbf{F}\neq 2$; $c=1$, 若 char $\mathbf{F}=2$.

(4) f 说是 Hermite 对称的, 若 $|\mathbf{F}|=q^2$, 且 $\mathbf{F}$ 带有 2 阶自同构 τ, τ 的不动点集是 $\mathbf{F}=GF(q^2)$ 的具有 q 个元素的子域 $\mathbf{F}_0=GF(q)$, 并且满足 $\forall u,v\in V$, 成立:

(i) $f(au,v)=af(u,v)$, $f(u,v+w)=f(u,v)+f(u,w)$.

(ii) $f(u,v)=f(v,u)^{\tau}$.

定义了数量积 f 的线性空间 V 叫做 度量空间, 常记作 (V,f).

在下文中, 在不至于发生误解的情况下, 我们也将 $f(x,y)$ 简记为 (x,y).

注意, 由以上定义, 我们可以直接得出以下几点简单结论:

(1) 若 f 为斜对称的, 且 char $\mathbf{F}=2$, 则 f 也是对称的.

(2) 若 f 为 Hermite 对称的, 则 $(u,av)=a^{\tau}(u,v)$.

(3) 若 f 为 V 上对称双线性型, Q 为与 f 相连带的二次型. 令 $X=\{x_i\mid 1\leq i\leq n\}$ 为 V 的一组基, 则 $Q(\sum\limits_i a_ix_i)=\sum\limits_i a_i^2Q(x_i)+\sum\limits_{i<j}ca_ia_j(x_i,x_j)$.

(4) 容易证明, 定义 2.1 中 (2),(3),(4) 任一种情况都意味着下列 (2.1) 式成立:

$$\text{对于 } u,v\in V,\quad (u,v)=0\Leftrightarrow(v,u)=0. \tag{2.1}$$

满足 (2.1) 中条件的向量对 (u,v) 说是互相垂直的, 记作 $u\perp v$. V 的子空间 U 和 W 说是互相垂直的, 若 $(u,w)=0,\forall u\in U,w\in W$; 若 U 和 W 互相垂直, 且 $U\cap W=\{0\}$, 记 $U+W=U\perp W$. 又记 $U^{\perp}=\{v\in V\mid (u,v)=0,\ \forall u\in U\}$. 若 $U=\langle u\rangle$, 则 $U^{\perp}$ 也记

作 $u^{\perp}$. $V^{\perp}$ 记作 $R(V)$, 并称之为 V 的 根. 我们说 f 非退化, 若 $R(V)=0$. 由线性代数可知, 若 U 为 V 的子空间, V 非退化, 则有 $\dim U^{\perp}+\dim U=n$.

定义 2.2 设 f 为 V 上数量积.

(1) f 说是 *正交型*. 若 f 非退化, 对称, 且当 char $\mathbf{F}=2$ 时 $(v,v)=0$, $\forall v\in V$. 这时 V 说是 $\mathbf{F}$ 上 *正交空间*.

(2) f 说是 *辛型*, 若 f 非退化, 斜对称. 这时 V 说是 $\mathbf{F}$ 上 *辛空间*.

(3) f 说是 Hermite 型, 若 f 非退化且为 Hermite 对称. 这时 V 说是 $\mathbf{F}$ 上 *酉空间*.

有时为了指明度量空间上的数量积, 我们常以 (V,f) 表辛空间或酉空间, 以 (V,Q) 表正交空间 (这里 Q 为与 V 上正交型 f 相连带的二次型). 正交空间, 辛空间, 酉空间都是 *非退化度量空间*.

下文凡说及度量空间, 若无特别说明, 总认为该空间属于定义 2.2 中三种情况之一.

设 V 为度量空间. 向量 $v\in V$ 说是 *迷向的*, 若 $f(v,v)=0$. 由定义可知, 若 f 为辛型, 则 V 中所有的向量都是迷向的. 若 char $\mathbf{F}=2$, 且 f 为正交型, V 中所有向量也都是迷向的. 设 U 为 V 的子空间. U 说是 *全迷向的*, 若 $U\subseteq U^{\perp}$, 这时有 $f(u,v)=0$, $\forall u,v\in U$; U 说是 *非退化的*, 若 $U\cap U^{\perp}=0$.

命题 2.3 *令 V 为度量空间, U 为 V 的子空间, 则*

(1) 若 U 非退化, 则 $V=U\perp U^{\perp}$.

(2) $(U^{\perp})^{\perp}=U$.

(3) 若 U 为全迷向的, 则 U 在 $U^{\perp}$ 中的补非退化.

(4) 若 U 全迷向, 则 $\dim(U)\leq n/2$.

证 (1), (2), (4) 是显然的. 我们仅需证明 (3): 令 $U^{\perp}=U\oplus H$, ($U\oplus H$ 表示 U 和 H 的直和), 则 $R(H)\oplus U\subseteq(U^{\perp})^{\perp}=U$. 这表明, $R(H)\subseteq U\cap H=\{0\}$, 即 H 非退化. □

在辛空间和酉空间中，迷向向量也叫做*奇异向量*. 若 V 为正交空间，向量 $v \in V$ 说是*奇异的*, 若 $Q(v) = 0$ (易知这时 v 必然是迷向的); V 的子空间 U 说是*全奇异的*, 若 U 是全迷向的，且 U 的每个元是奇异的. 实际上除非 V 为正交空间且 $\mathrm{char}\,\mathbf{F} = 2$, (全) 迷向与 (全) 奇异是一致的. 度量空间 V 中极大全奇异子空间的维数叫做 V 的 Witt *指数*.

有时我们还用到以下概念. 度量空间 (V, f) 到 (U, g) 的非退化线性变换 α 说是一个*相似变换*, 若成立: $f(u^\alpha, v^\alpha) = \lambda(\alpha)g(u, v)$, $\forall u, v \in V$, 其中 $\lambda(\alpha) \in \mathbf{F}^\#$, 且 $\lambda(\alpha)$ 与 u, v 的选择无关. 注意若 (V, f) 和 (U, g) 都是正交的，相应的二次型分别为 P 和 Q, 则还要求: $P(u^\alpha) = \lambda(\alpha)Q(u^\alpha)$. 这时也说 f 和 g 是相似的. α 说是 (V, f) 到 (U, g) 的*等距*, 若 α 为 (V, f) 到 (U, g) 的相似，且其中 $\lambda(\alpha) = 1$. 这时也说 V 和 U 是等距的，记作 $V \cong U$. 型 f 与 g 说是*等价的*, 若 V 与 U 等距. 度量空间 V 上全体等距构成一个群，我们以 $O(V, f)$ 或 $O(V, Q)$ 表示空间 V 的*等距群*. $O(V, f)$, $O(V, Q)$ 及其某些子群和商群都是本节前言中所提及的典型群.

令 $X = \{x_i \mid 1 \le i \le n\}$ 为 V 的一组基. 令 $J = J(X, f) = (J_{ij})$, 其中 $J_{ij} = (x_i, x_j)$, J 称为型 f 的对应矩阵. 注意 J 由型 f 唯一确定，且 J 非退化，即 $\det J \ne 0$ 当且仅当 f 非退化. 令 $\sigma \in GL(V)$, 且 σ 在 X 之下的矩阵为 $\mathrm{Mat}(\sigma) = (M_{ij})$. 则 $\sigma \in O(V, f)$ (或 $O(V, Q)$) $\Leftrightarrow \mathrm{Mat}(\sigma) J \mathrm{Mat}(\sigma)^{\tau T} = J$, 其中 $\mathrm{Mat}(\sigma)^\tau = (M_{ij}^\tau)$, A^T 表示矩阵 A 的转置，且 $\tau = 1$, 若 V 为正交空间或辛空间; τ 为域 $\mathbf{F}$ 的 2 阶自同构，若 V 为酉空间. 显然有 $\det \mathrm{Mat}(\sigma)^{1+\tau} = 1$.

下面我们讨论 (V, f) (或 (V, Q)) 中两种特殊的基. 利用这两种基我们可以把相应的空间分成一些等价类.

(V, f) (或 (V, Q)) 中的基 $X = \{v_i \mid 1 \le i \le n\}$ 说是 V 的一组*正交基*, 若其中所有的 v_i 都是非奇异的且两两互相正交. 若还成立 $(v_i, v_i) = 1$, 则 X 说是 V 的一组*标准正交基*.

引理 2.4 设 $\mathrm{char}\,\mathbf{F} \ne 2$, 则 $\forall a \in \mathbf{F}$, 可找到 x, y, 使得 $a = x^2 + y^2$.

证 令 $U = \{a^2 \mid a \in \mathbf{F}^{\#}\}$, 则 $\mathbf{F}^{\#} = U \cup Uk$, $k \notin U$. 若能找到 $a_0 = x_0^2 + y_0^2 \notin U$, 便有 $\mathbf{F}^{\#} = U \cup Ua_0$. 从而断言成立. 假定 $x^2 + y^2 \in U$, $\forall x, y \in \mathbf{F}^{\#}$ 这意味着 $L = \{0\} \cup U$ 为 $\mathbf{F}$ 的子域. 则由于 $|L| = (|\mathbf{F}| + 1)/2$, 立得矛盾. □

命题 2.5 假定 V 为域 $\mathbf{F}$ 上 n 维度量空间, $n \geq 2$, 则

(1) 若 V 不是辛空间, 则 V 中有非奇异向量.

(2) 若 V 为酉空间, 则 V 有标准正交基.

(3) 若 V 为正交空间且 $\mathrm{char}\,\mathbf{F} \neq 2$, 则 V 或有标准正交基, 或有正交基 $\{v_1, v_2, \cdots, v_n\}$, 其中 $(v_i, v_i) = 1$, $1 \leq i \leq n-1$, 且 $(v_n, v_n) = k$, k 为 $\mathbf{F}$ 中非平方元.

证 (1) 令 $v \in V^{\#}$, $u \in V \backslash v^{\perp}$. 不失一般性可假定 $(v,v) = 0 = (u,u)$, $(v,u) = 1$, 且若 V 正交, 还假定 $Q(v) = 0 = Q(u)$. 若 $\mathrm{char}\,\mathbf{F} \neq 2$, 则 $(v+u, v+u) = 2 \neq 0$, 即 $v+u$ 为非奇异向量.

若 $\mathrm{char}\,\mathbf{F} = 2$, 且 V 为酉空间, 取 $b \in \mathbf{F}^{\#}$ 使 $b \neq b^{\tau}$, 则 $(v+bu, v+bu) = b + b^{\tau} \neq 0$, 即 $v+bu$ 为非奇异向量. 若 $\mathrm{char}\,\mathbf{F} = 2$, 且 V 为正交空间, 则 $Q(v+u) = Q(v) + Q(u) + (v,u) = 1$, 特别地 $v+u$ 为非奇异向量.

(2) 我们先证 V 中有正交基. 由 (1), V 中有非奇异向量 v_1, 则 $V = v_1 \perp v_1^{\perp}$. 显然 $v_1^{\perp}$ 非退化. 由归纳假定, $v_1^{\perp}$ 中有正交基 $\{v_2, \cdots, v_n\}$, 从而 $\{v_1, v_2, \cdots, v_n\}$ 为 V 的一组正交基. 我们可以把所得正交基标准化: 由于范数映射为 $\mathbf{F}$ 到 $\mathbf{F}_0$ 上的满射, 故有 $b_i \in \mathbf{F}$, 使得 $(b_i v_i, b_i v_i) = b_i b_i^{\tau}(v_i, v_i) = 1$. 则 $\{b_i v_i | 1 \leq i \leq n\}$ 为一组标准正交基.

(3) 首先我们可以按照 (2) 证明中前一部分证明 V 中存在正交基. 因此要完成证明, 仅需证 V 的任意 2 维非退化子空间 U 中可找到向量 w, 使得 $(w,w) = 1$. 令 $\{v, u\}$ 为 U 的一组正交基, $(v,v) = (u,u) = k$, k 为 $\mathbf{F}$ 中非平方元. 由引理 2.4, 有 $x, y \in \mathbf{F}$, 使 $k(x^2 + y^2) = 1$. 令 $w = xv + yu$, 则 w 即为所求向量. □

以下我们讨论**双曲基**. 双曲基对于考察度量空间结构有着重要作用.

设 V 为一 $2m$ 维度量空间，$X = \{v_1\cdots, v_{2m}\}$ 是 V 的一组基，能使 $(v_i, v_i) = 0$, $(v_{2i-1}, v_{2i}) = 1$, 且

$$V = \langle v_1, v_2\rangle \perp \cdots \perp \langle v_{2m-1}, v_{2m}\rangle.$$

则说 X 是 V 的一组双曲基，$\{v_{2i-1}, v_{2i}\}$ 称为 V 中一个*双曲对*, $\langle v_{2i-1}, v_{2i}\rangle$ 叫做 V 中一个*双曲平面*. V 说是一个*双曲空间*, 若 V 可表为双曲平面之直和.

在命题 2.6 及下文的某些命题中，我们多次利用了范数映射的性质，有关内容请读者自行参阅以下教材.

N. Jacobson, *Basic Algebra*, Vol. I, 4.15. (pp.284–288.)

命题 2.6 (1) *若 V 为正交空间且 $\dim V \geq 3$ 或 V 为酉空间且 $\dim V \geq 2$, 则 V 中有迷向向量.*

(2) *若 V 为度量空间，且 V 中有奇异向量 v, 则可找到 $w \in V$, 使得 $\{v, w\}$ 为 $U = \langle v, w\rangle$ 中双曲对.*

证 (1) 首先假定 V 为正交空间且 $\dim V \geq 3$, 我们分别对 $\mathrm{char}\,\mathbf{F} \neq 2$ 和 $\mathrm{char}\,\mathbf{F} = 2$ 两种情况加以讨论.

若 $\mathrm{char}\,\mathbf{F} \neq 2$. 设 $\{v_1, v_2, \cdots, v_n\}$ 为 V 的一组正交基，则通过 $\mathbf{F}$ 中元加以适当调整，可假定 $(v_i, v_i) = 1$ 或 k, 这里 k 为 $\mathbf{F}^{\#}$ 中固定的非平方元. 由假定，可设 $(v_1, v_1) = (v_2, v_2)$. 则由命题 2.4, 有 $x, y \in \mathbf{F}^{\#}$, 使 $x^2 + y^2 = -(v_3, v_3)/(v_1, v_1)$. 从而 $xv_1 + yv_2 + v_3$ 为一迷向向量.

若 $\mathrm{char}\,\mathbf{F} = 2$. 设 $(v_1, \cdots, v_n)$ 为一组正交基，由于 $\mathbf{F} = \mathbf{F}^2$, 故若 $Q(v_1) \neq 0 \neq Q(v_2)$, 即可假定 $Q(v_1) = Q(v_2) = 1$, 从而 $Q(v_1 + v_2) = 0$, 即 $v_1 + v_2$ 为一奇异向量.

若 V 为酉空间. 由于 $n = \dim V \geq 2$, 故 V 中有标准正交基 $\{v_1, \cdots, v_n\}$. 设 $\mathrm{char}\,\mathbf{F} = 2$, 则 $v_1 + v_2$ 为迷向元. 若 $\mathrm{char}\,\mathbf{F} \neq 2$, 由于 $\mathbf{F}$ 在 $\mathbf{F}_0$ 上的范数 N 为满射，故可找到 $a \in \mathbf{F}$, 使得 $N(a) = a^{1+\tau} = -1$, 由此可得迷向向量 $v_1 + av_2$.

(2) 令 v 为 V 中奇异向量. 取 $u \in V\backslash v^{\perp}$, 不失一般性可假定 $(v, u) = 1$. 我们证明 $\langle v, u\rangle$ 为双曲平面. 若 u 奇异，则论断

成立. 假定 u 非奇异, 则 V 为酉空间或正交空间, 我们可以找到适当的 $a \in \mathbf{F}$ 使得 $(av+u, av+u) = a + a^\tau + (u,u) = 0$ 或 $Q(av+u) = Q(u) + ca = 0$(注意这里 c 与定义 2.1(3)(ii) 中一致). 令 $w = av+u$, 则 $\{v, w\}$ 即为所求的双曲对. □

利用命题 2.6, 可以得到如下有用的推论.

推论 2.7 令 U 为 V 的全奇异子空间, $R = \{r_i \mid 1 \le i \le m\}$ 为 U 的一组基, W 为 U 在 $U^\perp$ 中的补. 则有 V 的子集 $S = \{s_i \in V \mid 1 \le i \le m\}$ 能使 $\{r_i, s_i\}$ 为双曲平面 $U_i = \langle r_i, s_i \rangle$ 中的双曲对, 且 $W^\perp = \perp_{i=1}^m U_i$.

要证明推论 2.7, 只须注意 W 为非退化, 且 $\dim W^\perp = 2\dim U$.

推论 2.8 令 V 为任意度量空间, 且 $\dim V = 2$. 若 V 中有一奇异向量, 则 V 为双曲平面. 特别地, 在等价的意义下, 对于每种型, 带有奇异向量的 2 维非退化空间是唯一的.

由推论 2.8 可以很容易地证明如下的推论:

推论 2.9 两个辛空间等价, 当且仅当它们具有相同的维数.

2 维正交空间 V 上的二次型 Q 说是**定的**, 若 V 中不包含奇异向量. 这时也说 V 是定的.

命题 2.10 在等价的意义下, 域 $\mathbf{F}$ 上 2 维空间 V 上定二次型 Q 是唯一确定的. 进而, 在 V 中有基 $X = \{v, u\}$, 使:

(1) 若 $\operatorname{char}\mathbf{F} \ne 2$, 则 $(v,u) = 0$, $Q(v) = 1$, $Q(u) = -k$, k 为 $\mathbf{F}^\#$ 中的非平方元.

(2) 若 $\operatorname{char}\mathbf{F} = 2$, 则 $(v,u) = 1$, $Q(v) = 1$, $Q(u) = b$, 且 $P(t) = t^2 + t + b$ 为 $\mathbf{F}$ 上不可约多项式.

证 令 $K = \mathbf{F}(z)$ 为 $\mathbf{F}$ 上二次扩域, N 为 K 到 $\mathbf{F}$ 的范数映射, 则 $\{1, z\}$ 为 $\mathbf{F}$ 上二维空间的一组基. 由范数映射之定义可知, (K, N) 为定正交空间, 故我们仅需证 (V, Q) 等价于 (K, N).

由于 V 中不包含奇异向量，故若 char $\mathbf{F} \neq 2$, 则可选取基 $\{v, u\}$, 使 $(v, u) = 0$, $Q(v) = 1$, 且 $Q(u) = -k$, k 为 $\mathbf{F}^{\#}$ 中非平方元. 若 char $\mathbf{F} = 2$, 则可选取基 $\{v, u\}$, 使 $(v, u) = 1$, $Q(v) = 1$, $Q(u) = k$, 且 $P(t) = t^2 + t + k$, 为 $\mathbf{F}$ 上不可约多项式. 令 z 为多项式 $s^2 + s(v, u) + k$ 的根，其中 $(v, u) = 0$, 若 char $\mathbf{F} \neq 2$; $(v, u) = 1$, 若 char $\mathbf{F} = 2$. 令 $K = \mathbf{F}(z)$, 则 K 为 $\mathbf{F}$ 上二次扩域. 作 V 到 K 的映射 $\varepsilon : xv + yu \mapsto x + yz$, 则对于 char $\mathbf{F} \neq 2$, 我们有 $(xv + yu, xv + yu) = x^2 - ky^2 = N(x + yz)$, 而若 char $\mathbf{F} = 2$, 则有 $Q(xv + yu) = x^2 + xy + y^2 = N(x + yz)$. 由以上讨论可知，$\varepsilon$ 为 V 到 K 的等价. 这就证明了 (1) 和 (2) 成立. □

命题 2.11 令 (V, Q) 为正交空间，f 为与 Q 相连带的对称双线性型，则有

(1) 若 $\dim V = 2m + 1$, 则 char $\mathbf{F} \neq 2$. V 中有基 $\{v_i \mid 1 \leq i \leq n\}$, 能使 V 中超平面 $H = \langle v_i \mid 1 \leq i \leq 2m \rangle$ 为双曲空间，$H^{\perp} = \langle v_n \rangle$, 其中 $Q(v_n) = 1$ 或 δ, δ 为 $\mathbf{F}^{\#}$ 中非平方元.

(2) 若 $\dim V = n = 2m$, 则或者 V 为双曲空间，或者 V 中有基 $X = \{v_i \mid 1 \leq i \leq n\}$, 能使 $W = \langle v_i \mid 1 \leq i \leq n - 2 \rangle$ 为双曲空间，且 $W^{\perp} = \langle v_{n-1}, v_n \rangle$ 为 2 维定正交空间.

证 (1) 中双曲空间 H 和 (2) 中双曲空间 W 的存在性是命题 2.6 的直接结果. $H^{\perp}$ 是非退化的，故 (1) 中结论成立. 由于 $W^{\perp}$ 非退化，由命题 2.6 及命题 2.10 即得 (2) 中结论. □

在命题 2.11(1) 中，V 说是具有符号 $+1$, 记作 $\operatorname{sgn}(Q) = +1$, 若 $Q(v_n) = \delta$; V 说是具有符号 -1, 记作 $\operatorname{sgn}(Q) = -1$, 若 $Q(v_n) = 1$.

正交空间中极大全奇异子空间的维数，即该空间的 Witt 指数，记作 $\nu(V)$. 故在命题 2.11(1) 中 $\nu(V) = m$.

而在命题 2.11(2) 中，若 $\nu(V) = m - 1$, 便说 V 的符号为 $+1$; 若 $\nu(V) = m$, 则说 V 的符号为 -1.

Witt 引理是度量空间最重要的性质之一. 下面我们对此给出一个证明.

Witt 引理 令 V 为域 $\mathbf{F}$ 上度量空间. 令 U 和 W 都是 V 的子空间且有等距 $\alpha: U \to W$, 则 α 可扩充为 V 的一个等距.

证 我们对 V 的维数进行归纳.

(1) 假定 $0 \neq H \leq U$, H 非退化. 若 $H^{\perp} \cong (H^{\alpha})^{\perp}$, α 可扩充为 V 的等距. 特别地, 若 $H = H^{\alpha}$, α 可扩充为 V 的等距.

由假定, $V = H \oplus H^{\perp} = H^{\alpha} \oplus (H^{\alpha})^{\perp}$, 令 $\beta: H^{\perp} \mapsto (H^{\alpha})^{\perp}$ 为一等距. 由归纳假定, $(\alpha|_{U\cap H^{\perp}})\beta^{-1}$ 可扩充为 $H^{\perp}$ 的等距 γ, 即 $\alpha|_{U\cap H^{\perp}}$ 可扩充为等距 $\gamma\beta: H^{\perp} \mapsto (H^{\alpha})^{\perp}$, 从而 α 可扩充为 V 的一个等距 $\delta: \delta|_H = \alpha|_H$, $\delta|_{H^{\perp}} = \gamma\beta$.

(2) 若 $0 \neq H = R(U)$ 全奇异, 则 α 可扩充为 V 的一个包含 U 的非退化子空间 U' 的等距. 特别地, 若 $U = H^{\perp}$, 则 $U' = V$, 即 α 可扩充为 V 的等距.

记 $H = R(U)$, 则 $U = H \oplus M$. 其中 M 非退化或为 0. 令 $\{r_i \mid 1 \leq i \leq m\}$ 为 H 的一组基, 令 X 为 H 在 $H^{\perp}$ 中的补, 且 X 包含 M; X' 为 H^{α} 在 $(H^{\alpha})^{\perp}$ 中的补, 且 X' 包含 M^{α}. 由推论 2.7, 存在 $\{s_i \mid 1 \leq i \leq m\}$ 和 $\{s_i' \mid 1 \leq i \leq m\}$, 使 $X^{\perp}$ 和 $(X')^{\perp}$ 分别为双曲平面 $\langle r_i, s_i\rangle$ 和 $\langle r_i^{\alpha}, s_i'\rangle$ 之直和. 定义 $s_i^{\alpha} = s_i'$, 即可把 α 扩充到非退化子空间 $U' = \langle U, s_i | 1 \leq i \leq m\rangle$. 若 $U = H^{\perp}$, 则 $\dim U' = \dim U + m = \dim H^{\perp} + m = \dim H^{\perp} + \dim H = n$, 故有 $U' = V$.

(3) 若 $R(U)$ 中有全奇异子空间 $0 \neq H = H^{\alpha}$, 则 α 可以扩充为 V 的等距.

令 $L = H^{\perp}$, 则 U, W 均为 L 的子空间. 我们证明 α 可以扩充为 L 上一个等距 β. 令 $\overline{L} = L/H$, $\overline{f}(\overline{x}, \overline{y}) = f(x, y)$. 则型 f (或 Q) 导出一个型 $\overline{f}$(或 $\overline{Q}$), 且由 α 导出等距 $\overline{\alpha}: \overline{U} \to \overline{W}$. 由归纳假定, $\overline{\alpha}$ 可扩充为 $\overline{L}$ 的一个等距 $\overline{\beta}$. 令 X 为 L 的一组基, 且使 $X \cap H$ 和 $X \cap U$ 分别为 H 和 U 的基. 令 $\beta \in GL(V)$ 能使 $\beta|_U = \alpha$ 且 $\overline{x^{\beta}} = \overline{x}^{\overline{\beta}}$, $\forall x \in X - U$. 则有 $(x, y) = (\overline{x}, \overline{y}) = (\overline{x}^{\overline{\beta}}, \overline{y}^{\overline{\beta}}) = (x^{\beta}, y^{\beta})$, $\forall x, y \in X$, 这表明, β 为 L 上一个等距, 故由 (2), β, 从而 α 可扩充为 V 的一个等距.

(4) 若 V 为辛空间, 酉空间或为当 char $\mathbf{F} \neq 2$ 时, $\mathbf{F}$ 上的正交空间, 则 α 可扩充为 V 的一个等距.

若 U 退化, 则 $0 \neq R(U)$ 全奇异. 由 (2), α 可扩充为 V 的一个包含 U 的非退化子空间上的等距. 故可假定 U 非退化. 若 V 为辛空间, 则由 $U \cong W$, 便有 $\dim(U^{\perp}) = \dim(W^{\perp})$. 由推论 2.9 可知 $U^{\perp} \cong W^{\perp}$. 由 (1), 结论成立. 现假定 V 为酉空间或为正交空间且 char $\mathbf{F} \neq 2$. 我们对 U 的维数进行归纳. 假定 $\dim U = 1$. 由 (1), $U \neq W$. 令 $U = \mathbf{F}u$, $W = \mathbf{F}w$. 令 $K = U + W$. 定义 $\alpha' : u \mapsto u^{\alpha}$, $u^{\alpha} \mapsto cu$, 其中 $c = \frac{(u^{\alpha},u)}{(u,u^{\alpha})}$, 则 α' 为 K 上等距, 即有 $K^{\alpha'} = K$, 则由 (1), α 可扩充为 V 的等距. 现假定 $\dim U > 1$. 令 u_1 为 U 中非退化向量, 则 $U = \mathbf{F}u_1 \perp U_1$, $W = \mathbf{F}w_1 \perp W_1$, 其中 $w_1 = u_1^{\alpha}$, $W_1 = U_1^{\alpha}$. 又因 $V = \mathbf{F}u_1 \perp U_1 \perp U^{\perp} = \mathbf{F}w_1 \perp W_1 \perp W^{\perp}$, 故 $U_1 \perp U^{\perp} \cong W_1 \perp W^{\perp}$. 由归纳即得 $U^{\perp} \cong W^{\perp}$.

(5) 若 V 为正交空间, 且 char $\mathbf{F} = 2$, 则 α 可扩充为 V 上的等距.

我们先证明, 可将问题归结为如下情况: U 中有超平面 H 能使 $\alpha|_H = 1$. 选择 U 具有极小维数且等距 $\alpha : U \to W$ 不能扩充为 V 的等距. 令 H 为 U 的一个超平面. 由 U 的极小选择, $\alpha|_H$ 可扩充为 V 的一个等距 β, 以 $\alpha\beta^{-1}$ 代替 α, 即可假定 $\alpha|_H = 1$.

由 (1), H 中不包含非退化子空间, 故 H 全迷向.

假定 $U \neq W$, 取 $u \in U - H$, 则 $u^{\alpha} \neq u$, 记 $K = U + W$. 令 $\alpha' \in GL(V)$, 且能使: $v^{\alpha'} = v^{\alpha}, \forall v \in U$, $(u^{\alpha})^{\alpha'} = u$. 则 α' 在 K 上的限制为 K 上等距, α' 固定 $z = u + u^{\alpha}$, 从而 $H' = \langle H, z\rangle$ 为 K 中超平面, 且 $\alpha'|_{H'} = 1$. 现在我们假定 $U = W$. 显然 $\alpha|_U \neq 1$, 仍取 $u \in U - H$, 则 $u^{\alpha} = au + h$, $a \in \mathbf{F}^{\#}$, $h \in H$. α 作用在 $X = \langle u, h\rangle$ 上. 由 (1), $R(X) \neq 0$, 否则 α 可扩充为 V 的等距, 故 X 全迷向. 从而 $h \in R(U)$, 故 h 非奇异. 由于 $Q(u) = Q(u^{\alpha})$, 故 z 奇异, 且 $\langle z\rangle$ 为 X 中唯一的奇异点, (注意我们常把一维子空间称作点,) 因此是 α 不变的. 由 h 非奇异知 $z \notin H$. 又由 (3) 可知 $z \notin R(U)$. 不妨假定 $u = z$. 故可找到 $h' \in H - z^{\perp}$, α 作用在非退化子空间 $X' = \langle h', z\rangle$ 上, 故 α 可扩充为 V 上的等距, 矛盾. 这样, 我们就

完成了 Witt 引理的证明. □

推论 2.12 (1) 度量空间 V 上等距群, 在 V 的极大全奇异子空间集合上传递, 也在极大双曲子空间集合上传递.

(2) 正交空间 V 是它的极大双曲空间和一个定正交空间之直和, 且在等价的意义下, 这一分解是唯一的.

在以上讨论的基础上, 我们可以归纳出如下关于有限域上度量空间的分类定理.

定理 2.13 令 $\mathbf{F} = GF(q)$, $q = p^n$, (V, f) 为 $\mathbf{F}$ 上 n 维度量空间. 则

(1) 若 V 为辛空间, 则 n 为偶, V 为双曲的, 且在等价意义下 (V, f) 为唯一的.

(2) 若 V 为 n 维酉空间, 则在等价意义下 (V, f) 为唯一的.

(3) 若 n 为偶, 则在等价意义下, 恰有两个互不相同的正交空间, 其中之一具有符号 $+1$, 另一个具有符号 -1.

(4) 若 n 为奇, 则在等价意义下, 恰有两个互不相同的正交空间. 这两个正交空间是相似的, 且空间基域的特征为奇数.

现在我们讨论典型群. 我们引入一些符号来表示典型群及其某些子群: 设 V 为 $GF(q)$ 上 n 维辛空间, 则等距群 $O(V, f)$ 说是**辛群**, 记作 $Sp(V)$ 或 $Sp(n, q)$, 显然有 $Sp(V) \leq SL(V)$.

若 V 为 $GF(q^2)$ 上 n 维酉空间, 则 $O(V, f)$ 说是 **酉群**, 记作 $GU(V)$ 或 $GU(n, q)$, 记 $SU(V) = GU(V) \cap SL(V)$.

若 V 为 $GF(q)$ 上 n 维正交空间, 情况比较复杂:

若 $n = 2m + 1$, 则 $O(V, Q)$ 说是 $GF(q)$ 上 **正交群**, 记作 $O(2m+1, q)$. 记 $SO(V, Q) = O(V, Q) \cap SL(V)$, $\Omega(V, Q) = SO(V, Q)'$, $SO(V, Q)$ 和 $\Omega(V, Q)$ 分别记作 $SO(2m+1, q)$ 和 $\Omega(2m+1, q)$.

若 $n = 2m$, 则对应于 $\mathrm{sgn}(Q) = +1$ 或 $\mathrm{sgn}(Q) = -1$, 正交空间 (V, Q) 上可以定义两个互不同构的 **正交群**: $O_\varepsilon(2m, q)$, $\varepsilon = \pm 1$. 相应地, 我们可以定义 $SO_\varepsilon(2m, q)$ 和 $\Omega_\varepsilon(2m, q)$.

本节中以下部分, 我们以 G 表示 $O(V, f)$ 或 $O(V, Q)$, 以 L 表示 $O(V, f) \cap SL(V)$, 若 G 为辛群或酉群; 以 L 表示 $\Omega(2m + 1, q)$

或 $\Omega_\varepsilon(2m,q)$, 若 G 为正交群. 我们将证明, 若 G 为辛群, 酉群或特征 $\neq 2$ 的正交群, 则除个别例外, 总有 $L=L'$. 由此我们还将在 §3 中证明, 除上述例外, $L/Z(L)$ 均为单群. 特征为 2 的正交群, 也有类似结果, 但对其讨论时, 须利用 Clifford 代数作为工具, 限于篇幅, 我们略去了这方面的讨论.

在 §1 中我们看到在考察线性群时平延的作用. 典型群中平延也起到了类似的作用. 注意度量空间 V 上的平延本身又是等距, 这些平延均包含在 $O(V,f)\cap SL(V)$ 之中. 它们的性质和所在群的型有密切关系. 特征 $\neq 2$ 的正交群, 不包含平延, 我们将在其中定义另外两种特殊等距变换.

由于典型群作用在相应的度量空间上, 因此我们可以采用第 VII 章的符号: 设 $H\leq O(V,f)$ (或 $O(V,Q)$), U 是 V 的子空间. 记 $C_V(H)=\{v\in V \mid v^h=v,\forall h\in H\}$, $[U,H]=\langle -u+u^h \mid u\in U,h\in H\rangle$, $N_H(U)=\{h\in H \mid U^h=U\}$.

引理 2.14 (1) 若 $g\in G$, 则 $C_V(g)=[V,g]^\perp$.

(2) 若 $g\in G$, 则 g 为平延, 当且仅当 $[V,g]$ 为 V 中迷向点.

证 (1) 记 $U=C_V(g)$, 则 $\forall v\in V$, $u\in U$, $(u,-v+v^g)=(u,-v)+(u,v^g)=-(u,v)+(u^g,v^g)=0$. 这表明, $U\leq[V,g]^\perp$. 要证明等式成立, 仅需证 $\dim U=\dim V-\dim\,[V,g]=\dim\,[V,g]^\perp$. 作 V 到 $[V,g]$ 上的线性映射 $\varphi_g: v\mapsto -v+v^g$. $\mathrm{Ker}\ \varphi_g=U$. 故有 $\dim U=\dim V-\dim\,[V,g]=\dim\,[V,g]^\perp$.

由 (1) 及平延定义可立得 (2). □

令 $W=\langle w\rangle$ 为迷向点, 我们以 Δ_W 表示以 W 为中心的平延之集合. 若 W 为平延 t 的中心, 则说 $R=R_W=\langle\Delta_W\rangle$ 是 t 的根群, 有时也称为 G 中一个根群. 我们以 $\mathcal{C}$ 表示 V 中迷向点之集合.

定理 2.15 令 V 为域 $\mathbf{F}$ 上 n 维度量空间, t 为 V 上一平延, $W=\langle w\rangle$ 为 t 的中心, 则 $R^\#=\Delta_W$, $\forall v\in V$, $v^t=v+a_t(v,w)w$, 其中 a_t 为 $\mathbf{F}$ 中固定的元. 则下列诸情况之一成立:

(1) 假定 V 为 $\mathbf{F}=GF(q^2)$ 上酉空间，τ 为 $\mathbf{F}$ 上 2 阶自同构．则 $t\mapsto e^{-1}a_t$ 为 R 到 $\mathbf{F}_0=GF(q)$ 的同构，其中 $e\in\mathbf{F}^{\#}$, $e^{\tau}=-e$; V 中每个迷向点都是平延的中心，又 L 在平延的根群集合上传递．

(2) 若 V 为辛空间，则 V 中每个点都是平延的中心，$t\mapsto a_t$ 为 R 到 $\mathbf{F}$ 的加群的同构．G 在平延的根群集合上传递．

(3) 若 V 为正交空间，则 $\operatorname{char}\mathbf{F}=2$, $R=\langle t\rangle\cong Z_2$, W 非奇异，且 $a_t=Q(w)^{-1}$, V 中每个非奇异点都是唯一的平延的中心．

(4) 除去下列例外，总有 $R\le L'$: V 为酉空间或辛空间且 $n=2$, $q\le 3$; 或 V 为辛空间且 $n=4$, $q=2$.

证 假定 w 为 V 中迷向点．由于 V 非退化，故存在 $u\in V\backslash w^{\perp}$. 不妨假定 $(u,w)=1$. 由于 $V=\langle u\rangle\oplus w^{\perp}$, 故 $\forall v\in V$, 存在 $c\in\mathbf{F}$, $h\in w^{\perp}$ 使得 $v=cu+h$. 我们有 $(v,w)=c$. 令 $t\in GL(V)$ 为以 $\langle w\rangle$ 为中心的平延，则存在 $a_t\in\mathbf{F}$ 使得 $u^t=u+a_tw$. 由以上讨论可知，若 $v=cu+h$, 则 $v^t=v+a_t(v,w)w$. 由此易知 $t\in G$ 当且仅当 $(u,u)=(u^t,u^t)=(u+a_tw,u+a_tw)$, 即 $(u,a_tw)+(a_tw,u)=0$; 若 V 正交，还须 $Q(u)=Q(u^t)=Q(u+a_tw)$. 以下我们分别对各种不同型的空间进行讨论．

(1) 若 V 为酉空间，则应有 $a_t+a_t^{\tau}=0$. 我们先证明，此方程有解 e: 取 $d\in\mathbf{F}\setminus\mathbf{F}_0$, 其中 $\mathbf{F}_0=\{a\in\mathbf{F}\mid a^{\tau}=a\}$. 令 $e=d-d^{\tau}$, 则 e 便是以上方程的一个解．直接验证表明，$\forall b_t\in\mathbf{F}_0$, $a_t=eb_t$ 也是方程的解．即有 $t\in G$. 因此 $t\mapsto b_t$ 为 R 到 $\mathbf{F}_0$ 的加群的同构．上述讨论对任意迷向点 $\langle t\rangle$ 都适用，因此任意迷向点都是某些平延的中心．由 Witt 引理，G 在 C 上传递．

(2) 若 V 为辛群，则 $\forall a_t\in\mathbf{F}^{\#}$, 等式 $0=(u,a_tw)+(a_tw,u)$ 总成立，故 $\forall a_t\in\mathbf{F}^{\#}$, $t\in G$. 直接验证表明 $R\cong(\mathbf{F},+)$.

(3) 若 V 正交，取 $a_t\in\mathbf{F}^{\#}$, 则由 $0=(u,a_tw)+(a_tw,u)=2a_t$ 可知，$\operatorname{char}\mathbf{F}=2$. 进而由 $Q(u)=Q(u^t)=Q(u+a_tw)=Q(u)+(u,a_tw)+a_t^2Q(w)$, 得 $a_t=Q(w)^{-1}$. 特别地，w 非奇异．由于 a_t 由 w 唯一确定，故 $\langle w\rangle$ 是唯一一个平延的中心．这表明 $R\cong Z_2$.

(4) 取 $v \in C$ 使 $\{w, v\}$ 为一双曲对. 记 $U = \langle w, v\rangle$. 令 H 为由中心包含在 U 中的平延所生成的群. 由于 $W^{\perp} \le C_V(H)$, 故 H 忠实地作用在 U 上, 即 $H \le O(W, f)$, 则由下文中定理 2.24 及定理 2.25, $H \cong SL(2, q)$. 从而有 $R \le H = H' \le L'$, 除非 $q \le 3$, 这时有 $n > 2$.

首先设 V 为酉空间 $n \ge 3$, $q = 3$. 取 $U^{\perp}$ 中非奇异向量 z, 则 $Z = \langle w, v, z\rangle$ 为 3 维酉空间. 易知 $K := C_L(Z^{\perp}) \cong SU(Z)$. 显然 $K' \le L'$, 故仅需证 $R \le K'$. $\forall \eta \in R$, 可找到 $b \in \mathbf{F}$, 使 $w^{\eta} = w$, $z^{\eta} = z$, $v^{\eta} = v + bw$. 记 $\eta = \eta(b)$. 又令 $\lambda \in K$ 使 $w^{\lambda} = kw$, $z^{\lambda} = k^{q-1}z$, $v^{\lambda} = k^{-q}v$, $k^{q+1} \ne 1$. 这时 $[\lambda, \eta] = \eta(-k^{q+1}b + b)$. 随着 b 遍历 $\mathbf{F}$, $-k^{q+1}b + b$ 也遍历 $\mathbf{F}$. 这就证明了 $R \le L'$.

设 V 为辛空间, 且 $n \ge 4, q = 3$ 或 $n \ge 6, q = 2$. 令 Z 为包含 W 的非退化空间, 且令 $\dim Z = 4$, 若 $q = 3$; $\dim Z = 6$, 若 $q = 2$. 现在我们仅证明第一种情况, 第二种情况可以类似地证明. 我们有 $K := C_L(Z^{\perp}) \cong Sp(Z)$. 令 $X = \{w, u, z, v\}$ 为 Z 的一组基, 使得

$$J(X, f) = \begin{pmatrix} 0 & \mathbf{I}_m \\ -\mathbf{I}_m & 0 \end{pmatrix}.$$

设 $\eta, \zeta, \lambda \in Sp(V)$, $\mathrm{Mat}(\eta) = \mathbf{B}_{21}(1)$, $\mathrm{Mat}(\zeta) = \mathbf{B}_{32}(1)$, $\mathrm{Mat}(\lambda) = \mathbf{B}_{31}(-1)$. 简单计算表明, $\eta^{-1}\zeta^{-1}\eta\zeta = \lambda$. 由此立得 $R = \langle\lambda\rangle \le K' \le L'$. □

定理 2.16 令 V 为 $\mathbf{F} = GF(q^2)$ 上 n 维酉空间, $L = SU(V)$. 则

(1) L 由平延生成, 除非 $q = 2, n = 3$.

(2) $L' = L$, 除非 $q = 2$, $n \le 3$.

证 (1) 令 $\Gamma = \{v \in V \mid (v, v) = 1\}$. 令 H 为 G 中由全体平延所生成的群. 我们先证明 H 在 Γ 上传递. 令 $u, v \in \Gamma$, $W = \langle u, v\rangle$. 若 W 非退化, 则由下面的定理 2.24, $SU(W) \cong SL(2, q)$. 故可找到 $h \in H$ 使 $v = u^h$. 若 W 退化, 取 $0 \ne w \in R(W)$. 我们证

明，存在 $z \in \Gamma$, 使得 $\langle v,z\rangle$ 和 $\langle u,z\rangle$ 均非退化．若 $n>3$, 可取 $z \in \Gamma \cap v^{\perp} \cap u^{\perp}$. 这时 $\langle u,z\rangle$ 及 $\langle v,z\rangle$ 均非退化．若 $n=3$, 则由假定 $q>2$. 令 w, t 为 $v^{\perp}$ 的一组双曲基．不妨令 $u=v+w$, 则 $u^{\perp}=\langle w, v-t\rangle$. $\forall z \in u^{\perp}$, $z=aw+v-t$ 又 $\langle v,z\rangle \cap u^{\perp}=\langle aw-t\rangle$. 我们需选择适当的 a 使得 z 与 $aw-t$ 均非迷向．这相当于条件 $a+a^{\tau} \neq 1$ 或 0. 满足等式 $a+a^{\tau}=1$ 和 $a+a^{\tau}=0$ 的 a 构成 $\mathbf{F}_0$ 的一个陪集．由于 $|\mathbf{F}|>2$, 故 $\mathbf{F}$ 中至少包含 3 个 $\mathbf{F}_0$ 的陪集，故可选择适当的 a 使以上不等式成立．

(2) 这是 (1) 和定理 2.15 的直接结果．□

定理 2.17 令 V 为 $\mathbf{F}=GF(q)$ 上 $n=2m$ 维辛空间，$G=O(V,f)$, 则

(1) G 由平延生成；

(2) $G'=G$, 除非 $(n,q)=(2,2)$, $(2,3)$ 或 $(4,2)$;

(3) $|G|=q^{2^n}\prod_{i=1}^{n}(q^{2i}-1)$.

证　(1) 令 Ω 为 V 上双曲基之集合．令 H 为由 G 中平延所生成的子群．由于 $G_X=1$, $\forall X \in \Omega$, 故要证明 $H=G$, 仅需证 H 在 Ω 上传递．任取 $X, Y \in \Omega$, 我们证明有 $h \in H$, 能使 $Y=X^h$. 记 $X=\{u_i \mid 1 \le i \le n\}$, $Y=\{v_i \mid 1 \le i \le n\}$, 其中 $\{u_{2i-1}, u_{2i}\}$, $\{v_{2i-1}, v_{2i}\}$ 均为双曲对，$1 \le i \le m$. 由定理 2.25, 当 $n=2$ 时 $Sp(V) \cong SL(V)$, 从而结论成立．故假定 $n>2$, 又因 n 为偶数，故 $n>3$. 易知 H 在 $V^{\#}$ 上传递．因此可假定 $u_1=v_1$. 我们先证明可找到 $s \in H_{u_1}$ 使得 $v_2=u_2^s$. 由于 $(u_1,u_2)=(v_1,v_2)=1$, 故存在 $w \in u_1^{\perp}$ 使 $v_2=u_2+w$. 若 $u_2 \notin w^{\perp}$, 则有以 $\langle v\rangle$ 为中心的平延 s 使得 $v_2=u_2^s$, 且因 $v \in \langle u_1\rangle^{\perp}$, 故 $s \in H_{u_1}$. 若 $u_2 \in w^{\perp}$, 则如上可证 u_2, v_2 在 H_{u_1} 中均共轭于 u_1+u_2, 从而 u_2 和 v_2 互相共轭，因此我们又可假定 $u_2=v_2$. 由归纳假定 $H_{\langle u_1,u_2\rangle}$ 在 $\langle u_1,u_2\rangle^{\perp}$ 上的作用相当于 $Sp(\langle u_1,u_2\rangle^{\perp})$ 的作用，故有 $h \in H$, 使 $Y=X^h$.

(2) 这是 2.15(4) 的直接结果.

(3) 我们首先计算中有序双曲对 $\{x,y\}$ 的个数．注意第一向量 x 有 q^n-1 种选择．若 $\{x,y\}$ 是一个双曲对，则任意以 x 为第

一向量的双曲对具有形状 $\{x, y'\}$, 其中 $y' = y + z$, $z \in z^{\perp}$, 由于 $x^{\perp}$ 中有 q^{n-1} 个向量，故 z 有 q^{n-1} 种选择. 这表明有序双曲对个数为 $(q^n - 1)q^{n-1}$.

设 $\{x, y\}$ 为 V 中一个双曲对. 记 $W = \langle x, y\rangle$, $U = W^{\perp}$, 则 U 为 $2m-2$ 维辛空间. 设 $\{x', y'\}$ 为 V 中任意双曲对，则如下定义的线性映射 $\tau : x \mapsto x', y \mapsto y'$ 为 $\langle x, y\rangle$ 到 $\langle x', y'\rangle$ 的等距. 由 Witt 引理， τ 可扩充为 V 的等距. 这表明 G 在 V 中双曲对集合上传递，从而有 $|G| = (q^n - 1)q^{n-1}|K|$, 其中 $K = C_H(W) \cong Sp(W^{\perp}) \cong Sp(2m-2, q)$. 则用归纳法，即得结论. □

本节以下部分，除非特别说明，总假定 $\mathbf{F} = GF(q)$, char $\mathbf{F} \neq 2$, V 为 $\mathbf{F}$ 上有限维正交空间. 这时 $O(V, Q)$ 中不包含平延. 如下定义的反射变换，与其它情况下平延所起作用类似.

定义 2.18 设 V 为正交空间， $r \in O(V, Q)$ 说是 V 上反射, 若 $[V, r]$ 为 V 中一个点 $\langle u\rangle$. $\langle u\rangle$ 说是 r 的 **中心**. 为了表明反射的中心 $\langle u\rangle$, 也将 r 记作 r_u.

引理 2.19 设 V 为正交空间，则

(1) 若 r 为 V 上反射，则 r 为对合， $[V, r]$ 非奇异.

(2) 设 $U = \langle u\rangle$ 为 V 中非奇异点，则有唯一的以 U 为中心的反射 r_u, 且 $v^{r_u} = v - \frac{2(v,u)}{Q(u)}u$, $\forall v \in V$.

证 (1) 令 r 为 V 上反射，则 $[V, r] = \langle v\rangle$ 为一个点，从而 $C_V(r) = v^{\perp}$ 为一超平面. 由定理 2.15(3), r 非平延，故 $v \notin v^{\perp}$, 特别地 $[V, r]$ 非奇异. 又 $v^r = av$, 其中 $1 \neq a \in \mathbf{F}^{\#}$, 故 $Q(v) = Q(v^r) = Q(av) = a^2Q(v)$. 从而 $a = -1$, 故 r 为一对合.

(2) 令 $U = \langle u\rangle$ 为 V 中一个非奇异点，则 $V = U \oplus U^{\perp}$. 故由 (1), 至多有一个以 U 为中心的反射. 直接验证表明，线性变换 r_u 便是所求的反射. □

记 $O(V, Q) = O(n, q)$, $O(V, Q) \cap SL(V) = SO(n, q)$. 由引理 2.19(2) 易知, 若 r 为 V 上反射, 则 $\det r = -1$, 特别地 $r \notin SO(n, q)$.

引理 2.20 令 V 为正交空间, $G=O(V,Q)$, 则 G 由反射生成.

证 令 η 为 V 上正交变换, u 为 V 中一个非奇异向量, 则向量 $u-u^{\eta}$ 和 $u+u^{\eta}$ 二者中必有一个是非奇异的, 记这一非奇异向量为 $w=u+\varepsilon u^{\eta}$, $\varepsilon=+1$ 或 -1. 令 r_w 为以 $W=\langle w\rangle$ 为中心的反射, $\eta'=r_w\eta^{-1}$, 则有 $u^{\eta'}=-\varepsilon u$, 特别地, $n-1$ 维非退化正交空间 $U^{\perp}$ 是 η'-不变的. 则用归纳法可设, $\eta'|_{U^{\perp}}=\bar{r}_{w_1}\cdots\bar{r}_{w_k}$, 其中 $\bar{r}_{w_i}$ 为 $U^{\perp}$ 中以非奇异点 $\langle w_i\rangle$ 为中心的反射. 由于 $w_i\perp u$, 故 V 上以 $\langle w_i\rangle$ 为中心的反射 r_{w_i} 固定 u, 这表明 $\bar{r}_{w_i}$ 为 r_{w_i} 在 $U^{\perp}$ 上的限制, 从而 $\eta''=\eta' r_{w_k}\cdots r_{w_1}$ 在 $U^{\perp}$ 上平凡作用. 又 $u^{\eta'}=u^{\eta'}=u$ 或 $-u$. 若 $u^{\eta'}=u$, 则 $\eta''=1$, 而若 $u^{\eta''}=-u$, 则 $\eta''=r_u$. 在任一种情况下 η' 都是反射之积, 这就证明了 $\eta=\eta'^{-1}r_w$ 是反射之积. □

在正交群中, 我们还可以定义另一种由迷向点决定的变换, 其性质与平延更为接近. 设 $\{x,y\}$ 为一双曲对. 则 $V=\langle x\rangle^{\perp}\oplus\langle y\rangle$. 对于 $u\in U=\langle x,y\rangle^{\perp}$, 可定义 V 上一个线性变换 $\rho_{x,u}$, 使得:

$$z^{\rho_{x,u}}=z+(z,u)x,\ \forall z\in\langle x\rangle^{\perp},\ y^{\rho_{x,u}}=-Q(u)x+y-u. \tag{2.2}$$

命题 2.21 设 (V,Q) 为正交空间, $\{x,y\}$ 为 V 中一个双曲对, $u\in U=\langle x,y\rangle^{\perp}$, $\rho_{x,u}$ 满足 (2.2) 中条件, 记 $H_x=\langle\rho_{x,u}\mid u\in U\rangle$, 则 (1) $\rho_{x,u}\in SO(V,Q)$; (2) $x^{\rho_{x,u}}=x$; (3) $\rho_{x,u_1}\rho_{x,u_2}=\rho_{x,u_1+u_2}$; (4) $\rho_{x,u}=1\Leftrightarrow u=0$; (5) $\eta^{-1}\rho_{x,u}\eta=\rho_{x^{\eta},u^{\eta}}$; (6)$\rho_{ax,u}=\rho_{x,au}$; (7) 若 $\eta\in\operatorname{Stab}x$, 则 $\eta^{-1}\rho_{x,u}\eta=\rho_{x,u^{\eta}}$. 由此可知 $H_x\lhd\operatorname{Stab}x$; (8) $H_x\cong(U,+)$, 特别地, H_x 为可换群.

本命题中 (1)–(8) 均可由 $\rho_{x,u}$ 之定义得出.

命题 2.22 设 V 为正交空间, C 为 V 中全体迷向点的集合. 则 $\forall x\in C$, H_x 在集合 $\Lambda=\{y\in C\mid(x,y)=1\}$ 上传递.

证 设 $y,z\in\Lambda$, 则 $V=\langle x\rangle\oplus\langle y\rangle\oplus U$, 其中 $U=\langle x,y\rangle^{\perp}$, 从而 $z=ay+bx+u$, $a,b\in\mathbf{F},u\in U$. 由 $(z,x)=1$, $Q(z)=0$. 故 $a=1$,

$b+Q(u)=0$. $z=y-Q(u)x+u$. 由 $\rho_{x,-u}$ 之定义即得 $z=y^{\rho_{x,-u}}$. 由此立得结论. □

定理 2.23 (1) 设 (V,Q) 为正交空间, 且 $\dim V \geq 3$, 令 $G=O(V,Q)$, $L=SO(V)$, 则 $G'=L'$.

(2) 令 (V,Q) 为一正交空间, $\Omega=\Omega(V,Q)$. 则 $\Omega=\Omega'=O(V,Q)'$, 除非 $\dim V=4$, $\mathrm{sgn}(Q)=+1$; 或 $n=3$, $|\mathbf{F}|=3$.

证 (1) 我们首先证明 G' 由反射的换位子 $r_u^{-1}r_v^{-1}r_ur_v=(r_ur_v)^2$ 生成. $\forall\eta\in G$, 我们有 $\eta^{-1}r_u\eta=r_{u^\eta}$, 故全体 $(r_ur_v)^2$ 生成 G 的一个正规子群 H. 商群 G/H 由全体形如 r_uH 的陪集生成. 由于生成元可换, 故 G/H 可换, $G'\leq H$. 又由换位子之定义, 反向不等式成立, 故有 $G'=H$.

下面我们证明, 任何 $(r_ur_v)^2\in L'$. 若 n 为奇, 则 $-r_u,-r_v\in L$, 且 $-1\in Z(O(V,Q))$, 从而有 $(r_ur_v)^2=[r_u,r_v]=[-r_u,-r_v]\in L'$. 现假定 n 为偶, 且 $n\geq 4$. 令 $U=\langle u,v\rangle$, 我们断言存在 $w\in U^\perp$, $Q(w)\neq 0$. 若否, 则 $U^\perp$ 为全迷向, 从而 $U^\perp\subseteq U^{\perp\perp}=U$, 矛盾. 由反射之基本性质, $w^{r_u}=w$, $r_u^{-1}r_wr_u=r_{w^{r_u}}=r_w$, 即有 $r_ur_w=r_wr_u$. 类似地, 还有 $r_vr_w=r_wr_v$. 由以上讨论即得 $[r_u,r_v]=[r_ur_w,r_vr_w]\in L'$.

(2) 由 (1) 只需证明 $\Omega=\Omega'$. 为此仅需证若 $\{x,y\}$ 为 V 中任意双曲对, 则 $\rho_{x,u}\in\Omega'$, $\forall u\in\langle x,y\rangle^\perp:=U$. 令 $\tau,\eta_a\in O_{x,y}=\{r_{u'}\mid u'\in\langle x,y\rangle\}$ 使 $x^\tau=y$, $y^\tau=x$; $x^{\eta_a}=ax$, $y^{\eta_a}=a^{-1}y$. 易知 $\tau\eta_a^{-1}\tau\eta_a=\eta_{a^2}\in\Omega$. 假定 $u\in U$. 我们有

$$\eta_{a^2}^{-1}\rho_{x,u}^{-1}\eta_{a^2}\rho_{x,u}=\rho_{a^2x,-u}\rho_{x,u}=\rho_{x,-a^2u}\rho_{x,u}=\rho_{x,(-a^2+1)u}.$$

若 $q\geq 4$, 可选择 $a\in\mathbf{F}^\#$, 使 $a^2\neq 1$, 以 v 代替 $(-a^2+1)u$, 可知 $\rho_{x,v}\in\Omega'$. 由于 v 随着 u 遍历 U, 即有 $\Omega'=\Omega=G'$.

若 $q=3$, 则由假定 $n\geq 4$, 且若 $n=4$, 则 $\nu(v)=1$. 由于 U 中有正交基, 则由公式 $\rho_{x,u_1}\rho_{x,u_2}=\rho_{x,u_1+u_2}$ 可知, 我们仅需证明, 对任意 $u\in U$, $Q(u)\neq 0$, 必有 $\rho_{x,u}\in\Omega'$. 若 $n=4$, $\nu=1$, U 为 2 维非迷向子空间, 故可找到 $v\in U$, 使 $\{u,v\}$ 为一组正交基. 由于

U 不可能为双曲的，故有 $Q(u)=1=Q(v)$ 或 $Q(u)=-1=Q(v)$. 若 $n\geq 5$, 则 U 非退化且 $\dim U\geq 3$. 故 $\dim(u^{\perp}\cap U)\geq 2$, 且 $u^{\perp}\cap U$ 非退化. 故可找到 $v\perp u$, 使 $Q(v)=Q(u)$. 因此存在 $\tau\in G$, 使 $x^{\tau}=x$, $u^{\tau}=-v$, $v^{\tau}=u$. 故有 $x^{\tau^2}=x$, $u^{\tau^2}=-u$, $v^{\tau^2}=-v$; 从而得

$$\tau^{-2}\rho_{x,u}^{-1}\tau^2\rho_{x,u}=\rho_{x,u}\rho_{x,u}=\rho_{x,2u}=\rho_{x,u}^{-1}.$$

现证明 $\tau^2\in G'$. 我们以 g_i 表示 V 上反射，则 $g_i^2=1$. 我们证明 $\forall g\in G$, $g^2\in G'$. 假定 $g=g_1g_2\cdots g_k$, $g^2=g_1g_2\cdots g_kg_1g_2\cdots g_k=g_1g_2\cdots g_{k-1}g_1g_2\cdots g_{k-1}(g'^{-1}g_k^{-1}g'g_k)$, 其中 $g'=g_1g_2\cdots g_{k-1}$. 对 k 归纳可知 $g^2\in G'$. 这表明 $\tau^2\in G'\subseteq\Omega$, 从而有 $\rho_{x,u}\in\Omega'$. 这就证明了 $\Omega=\Omega'=G'$. □

在定理 2.17 中我们计算了 $Sp(2m,q)$ 的阶，用类似方法，我们也可以求得其他典型群的阶. 我们不再详加讨论，而仅列举有关结果.

$$\begin{aligned}
|GU(n,q)| &= q^{n(n-1)/2}(q+1)\prod_{i=2}^{n}(q^i-(-1)^i),\\
|O(2m+1),q)| &= 2q^{m^2}\prod_{i=1}^{m}(q^{2i}-1),\\
|O_{\varepsilon}(2m,q)| &= 2q^{m(m-1)}(q^m-\varepsilon)\prod_{i=1}^{m}(q^{2i}-1).
\end{aligned}$$

对于正交群，总有 $|O(V,Q)/SO(V,Q)|=2$.

作为本节的结尾，我们讨论一些低维典型群的性质和结构.

定理 2.24 $SU(2,q)\cong SL(2,q)$.

证　设 $\mathbf{E}=GF(q^2)$, $\mathbf{F}=GF(q)$, V 为 $\mathbf{E}$ 上 2 维酉空间, $\{u,v\}$ 为 V 中一组双曲基. $L=SL(V)\cong SL(2,q^2)$, $G=SU(V)=SU(2,q)$, $H=SL(2,q)$. 我们证明，在 $\{u,v\}$ 之下，我们有

$$SU(2,q)=\left\{\begin{pmatrix}c_1 & ed_1\\ ec_2 & d_2\end{pmatrix}\middle| e\in\mathbf{E}, e^{q-1}=-1, c_i,d_i\in\mathbf{F}\right\}.$$

设 $\alpha = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in L$, 则 $\alpha \in G$, 当且仅当下列关系式成立：(1) $a_1b_2 - a_2b_1 = 1$; (2) $a_1b_1^q + b_1a_1^q = 0 = a_2b_2^q + b_2a_2^q$; (3) $a_1b_2^q + a_2b_1^q = 1$.

注意在 $\mathbf{E}$ 中，满足条件 $x^{q-1} = -1$ 的元构成 $\mathbf{F}$ 在 $\mathbf{E}$ 的一个陪集 $e\mathbf{F}$, 其中 e 为 $\mathbf{E}$ 中一个固定元，能使 $e^{q-1} = -1$. 特别地，若 char $\mathbf{F} = 2$, 则有 $e \in \mathbf{F}$, 即 $e\mathbf{F} = \mathbf{F}$.

若 $a_1 = 0$, 则有 $a_2b_1 = -1$, $a_2b_1^q = 1$, 由此得 $b_1^{q-1} = -1$, 故有 $a_2 = b_1^{-1} \in e\mathbf{F}$. 若 $b_2 \neq 0$, 由 (2) 立知 $b_2 \in \mathbf{F}$. 类似地，若 $b_1 = 0$, 则可证：$b_2 = a_1^{-1} \in \mathbf{F}$. 这时若 $a_2 \neq 0$, 则 $a_2 \in \mathbf{F}$.

现假定 $a_1 \neq 0 \neq b_1$. 由 (2) 有 $b_1^{q-1} + a_1^{q-1} = 0$, 代入 (3) 即得 $a_1^{q-1} = 1$. 从而由 (1) 立知 $b_2 \in \mathbf{F}$, $a_2 \in e\mathbf{F}$.

反之，若 $\alpha = \begin{pmatrix} c_1 & ed_1 \\ ec_2 & d_2 \end{pmatrix}$, 其中 $c_i, d_i \in \mathbf{F}$, 且 $\det\alpha = 1$, 则 $\alpha \in G$.

作 G 到 H 的映射 $\eta : \begin{pmatrix} c_1 & ed_1 \\ ec_2 & d_2 \end{pmatrix} \mapsto \begin{pmatrix} c_1 & d_1 \\ e^2c_2 & d_2 \end{pmatrix}$. 显然 η 是 G 到 H 的一个同构映射. □

我们还有如下结果

定理 2.25 $SL(2,q) \cong Sp(2,q)$.

定理 2.25 的证明留给读者.

定理 2.26 $Sp(4,2) \cong S_6$.

证 设 V 为 $GF(2)$ 上 4 维辛空间. 我们考察 V 的子集 $S = \{v_i \in V | 1 \leq i \leq 5, (v_i, v_j) = 1, i \neq j\}$. 由于 $\langle v_1, v_2\rangle$ 为双曲平面，故有 $V = \langle v_1, v_2\rangle \perp H$, 其中 H 为 2 维辛空间. 特别地，H 中有双曲对 $\{x_1, x_2\}$. 注意 $\{x_1, x_2\}$ 为 H 的一组基. 则必有 (不考虑顺序):

$$v_2 = v_1 + v_2 + x_3, v_4 = v_1 + v_2 + x_4, v_5 = v_1 + v_2 + x_3 + x_4,$$

且每个双曲对 $\{v_1, v_2\}$ 恰好可以补充为唯一一个集合 $\mathcal{S}$, 每个 $\mathcal{S}$ 中包含 20 个双曲对. 易知 V 中恰有 120 个双曲对, 故 V 中向量可构成 6 个 $\mathcal{S}$.

由定理 2.15, $Sp(4,2)$ 在 $V^{\#}$ 上传递作用, 故 $Sp(4,2)$ 在诸 $\mathcal{S}$ 之集合上传递, 从而有 $Sp(4,2)$ 到 S_6 的同态 φ. 设 $K = \mathrm{Ker}\,\varphi$. $V = \langle v_1, v_2\rangle \perp \langle x_3, x_4\rangle$, $(v_1, v_2) = (x_3, x_4) = 1$. 令

$$S = \{v_1, v_2, v_1 + v_2 + x_3, v_1 + v_2 + x_4, v_1 + v_2 + x_3 + x_4\},$$

$$S' = \{x_3, x_4, x_3 - x_4 + v_1, x_3 + x_4 + v_2, x_3 + x_4 + v_1 + v_2\}.$$

K 保持 S 和 S' 不变, 从而保持集合 $S \cap S' = \{v_1 + v_2 + x_3 + x_4\}$ 不变, 即 $v_1 + v_2 + x_3 + x_4$ 被 K 所固定. 由于 $Sp(4,2)$ 在 $V^{\#}$ 上传递, 且 $K \trianglelefteq Sp(4,2)$, 故 $K = 1$, 即 φ 为同构嵌入. 又由于 $|Sp(4,2)| = |S_6|$, 故有 $Sp(4,2) \cong S_6$. □

定理 2.27 (1) $SO_{+1}(2,q) \cong Z_{q-1}$;

(2) $SO_{-1}(2,q) \cong Z_{q+1}$.

证 (1) 设 V 为 2 维正交空间, $\mathrm{sgn}(V) = +1$, $\{v_1, v_2\}$ 为其一组双曲基. 由于 $(av_1 + bv_2, av_1 + bv_2) = 2ab$, 故 $v \in V$ 为迷向向量, 当且仅当 v 具有形状 av_1 或 bv_2, $a, b \in \mathbf{F}$. $\forall g \in SO(V, Q)$, 必有 $v_1^g = av_2$, $v_2^g = bv_1$ 或 $v_1^g = av_1$, $v_2^g = bv_2$. 在第一种情况下有 $ab = (v_1^g, v_2^g) = (v_1, v_2) = 1$, 由此得 $\det g = -1$, 矛盾. 在第二种情况下, 有 $\det g = ab = (v_1^g, v_2^g) = (v_1, v_2) = 1$. 由此立得结论.

(2) 令 (V, Q) 为 $\mathbf{F} = GF(q)$ 上 2 维定正交空间. V 中有正交基 $\{v_1, v_2\}$, 其中 $Q(v_1) = 1$, $Q(v_2) = -k$. 则 $K = \mathbf{F}(z)$, 其中 $z^2 = -k$, 为 $\mathbf{F}$ 上二次扩域. 则由命题 2.10 的证明过程可知, (K, N) 为上 2 维定正交空间, 其中 N 为 K 到 $\mathbf{F}$ 上的范数映射. 映射 $\varepsilon : av_1 + bv_2 \mapsto a + bz$ 为 V 到 K 的等距. 故我们仅需证明 $SO(K, N) \cong Z_{q+1}$.

令 $T = \{t_a \mid x^{t_a} = ax, \forall x \in K;\ N(a) = 1\}$. 显然 $T \subseteq SL(K)$ 且 $T \cong Z_{q+1}$. 我们证明 $T = SO(K, N)$. 首先 $\forall t_a \in T$, $N(x^{t_a}) = N(ax) = N(a)N(x) = N(x)$, 故 t_a 为正交变换. 反之

$\forall g \in SO(K,N)$, 若 $1^g = a$, 则有 $N(a) = N(1) = 1$. 令 $h = gt_a^{-1}$, 则 $h \in SO(K,N)$, 且 $1^h = 1$. 设 $z^h = b + cz$, 其中 $z \in K$, $b, x \in \mathbf{F}$, 则有

$$\begin{aligned} 0 &= (1,z) = (1^h, z^h) = N(1^h + z^h) - N(1^h) - N(z^h) \\ &= (1+b)^2 - kc^2 - 1 - b^2 + kc^2 = 2b. \end{aligned}$$

从而得 $c = \det h = 1$. 这表明 $g = t_a$. 这就证明了 $SO(K,N) \cong T \cong Z_{q+1}$. □

§3. 射影空间和射影群

本节中我们介绍射影几何的基本概念, 还将证明有限域上射影典型群的单性.

令 V 为 $\mathbf{F}$ 上 $n+1$ 维向量空间, $\mathcal{P}$ 为 V 上全体 1 维子空间之集合. $\mathcal{P}$ 的一个子集 α 说是 $\mathcal{P}$ 的一个子空间, 若有 V 的子空间 U, U 的全体 1 维子空间之集合恰为 α. 我们规定 $\dim\alpha = d$, 若 $\dim U = d+1$. 集合 $\mathcal{P}$ 连同如上定义的全体子空间叫做 V 上 n 维 *射影空间*, 或者叫做 $\mathbf{F}$ 上 n 维射影空间. $\mathcal{P}$ 也记作 $PG(n,q)$ 或 $PG(V)$. 由定义可知, $\mathcal{P}$ 的元为 0 维 子空间. 通常, 我们用几何术语称呼 $\mathcal{P}$ 的子空间, 0 维子空间称为 *点*, 1 维子空间称为 *线*, 2 维子空间称为 *平面*, $n-1$ 维子空间称为 *超平面*. 空集为 -1 维子空间且对应于 V 的子空间 $\{0\}$. 设 π 为 $\mathcal{P}$ 中超平面, P 为 $\mathcal{P}$ 中一个点, 若 $P \in \pi$, 则说 π 与 P 相关联.

对于 $\mathcal{P}$ 中点 P, 可找到 $u \in V$, 使 $P = \langle u \rangle = \mathbf{F}u$. u 说是 P 的生成向量. 通常 $\langle u \rangle$ 也记作 $P(u)$, 显然 $\forall a \in \mathbf{F}^{\#}$, $P(au) = P(u)$. $\mathcal{P}$ 中点 $P_1, P_2, \cdots, P_r$ 说是无关的, 若 $P_i = \langle u_i \rangle$, $\forall i \in \{1, \cdots, r\}$, 且 $u_1, \cdots, u_r$ 无关.

若 V 为度量空间, 则相应的射影空间 $\mathcal{P}$ 说是 *射影度量空间*, 例如 *射影辛空间*, *射影酉空间*, *射影正交空间* 等.

设 α 和 β 分别为 V 上射影空间 $\mathcal{P}$ 的两个子空间. 则 α 与 β 分别对应 V 的两个子空间 U 和 W. 我们以 $\alpha \cap \beta$ 表示既包含在 α 中又包含在 β 中最大的子空间. 不难看出, $\alpha \cap \beta$ 与集合 α

和 β 的交是一致的，我们也就把 $\alpha\cap\beta$ 称为 α 和 β 的交. 我们还以 $\alpha\cup\beta$ 表示既包含 α 又包含 β 的最小的子空间. 易知 $\alpha\cup\beta$ 对应于 V 的子空间 $U+W$, 我们把 $\alpha\cup\beta$ 称为 α 和 β 的联. 若 $\{\alpha_i \mid 1\le i\le k\}$ 为 $\mathcal{P}$ 中一组子空间，我们把 $\mathcal{P}$ 的包含所有 α_i 的最小子空间叫做由 $\{\alpha_i \mid 1\le i\le k\}$ 所张成的子空间，并记之为 $\alpha_1\cup\cdots\cup\alpha_k$. 若对于任意 i, 以 U_i 表示 α_i 对应的 V 的子空间，则 $\alpha_1\cup\cdots\cup\alpha_k$ 对应于 V 的子空间 $U_1+\cdots+U_k$. 对任意二个子空间 α,β, 我们有 $\dim\alpha+\dim\beta=\dim(\alpha\cup\beta)+\dim(\alpha\cap\beta)$.

设 α 为 V 中 1 维子空间，则有 $0\ne u\in V$, 能使 $\alpha=\langle u\rangle=\langle\lambda u\rangle$, $\lambda\in\mathbf{F}^{\#}$. 因此 $\mathcal{P}$ 中点便是由 $V^{\#}$ 上的等价关系 "$\sim$": $u\sim v\Leftrightarrow v=\lambda u$, $\lambda\in\mathbf{F}^{\#}$, 所定义的等价类. 故射影空间 $\mathcal{P}$ 中的点 P_i 可由属于等价类 P_i 的向量 u_i 作为其代表元. 因此与 $\mathcal{P}$ 中点 P_i 有关的问题，可以转化为关于 V 中向量 u_i 的问题加以处理. 度量空间中一些概念也可引入射影空间. 若 $P,Q\in\mathcal{P}$, 其中 $P=\langle x\rangle$, $Q=\langle y\rangle$. P 说是 *迷向的*, 若 $(x,x)=0$, 否则说是 *非迷向的*; P,Q 说是互相垂直，记作 $P\perp Q$, 若 $(x,y)=0$; $\{P,Q\}$ 说是一个 *双曲对*, 若 $(x,x)=(y,y)=0$ 且 $(x,y)\ne 0$. 这种情况下我们常假定 $(x,y)=1$.

我们以 $\mathcal{PC}$ 表示射影空间 $\mathcal{P}$ 中全体迷向点之集合，$\mathcal{PC}$ 说是 $\mathcal{P}$ 中 *二次锥面*.

命题 3.1 *令 $P_0,P_1,\cdots,P_d$ 为 $\mathcal{P}$ 中 $d+1$ 个点，并令 $\alpha=P_0\cup P_1\cup\cdots\cup P_d$. 令 $0\ne u_i\in V$ 为点 P_i 之代表元，则 $\dim\alpha=d$ 当且仅当向量 $u_0,u_1,\cdots,u_d$ 无关. α 对应于 V 中由 $u_0,u_1,\cdots,u_d$ 所生成的子空间.*

本命题之结论可由线性代数的有关结果直接得出.

定义 3.2 令 $\mathcal{P}$ 为 n 维射影空间，$\mathcal{P}$ 中点集 $\Sigma=\{P_0,P_1,\cdots,P_n\}$ 说是 $\mathcal{P}$ 的一个 *框架*, 若 $P_0,P_1,\cdots,P_n$ 无关. $\mathcal{P}$ 中点集 $\Lambda=\{P_0,P_1,\cdots,P_{n+1}\}$ 说是 $\mathcal{P}$ 的一组基，若 Λ 中任意 $n+1$ 个点为一个框架.

利用基可在 $\mathcal{P}$ 上建立坐标系：设 $\Lambda=\{P_0,P_1,\cdots,P_{n+1}\}$ 为 $\mathcal{P}$ 的一组基. 令 $P_i=\langle u_i\rangle$, $i=0,1,\cdots,n+1$. 则对任意 $t\in\mathbf{F}^{\#}$ 可

找到 $a_0, a_1, \cdots, a_n$ 使 $tu_{n+1} = a_0u_0 + a_1u_1 + \cdots + a_nu_n$. 注意这时 $a_i \neq 0$, $\forall i = 0, 1, \cdots, n$, 故 $\forall P = \langle u \rangle \in \mathcal{P}$, 可找到 $t_0, t_1, \cdots, t_n$, 使 $u = t_0a_0u_0 + t_1a_1u_1 + \cdots + t_na_nu_n$. $(t_0, t_1, \cdots, t_n)$ 说是 P 在基 Λ 之下的齐次坐标. 选定 t, 则 $(t_0, t_1, \cdots, t_n)$ 是唯一确定的.

设 $\Sigma = \{P_0, P_1, \cdots, P_n\}$ 为 $\mathcal{P}$ 的一个框架, u_i 为 P_i 之代表元, $1 \leq i \leq n$, 则向量 $u_0, u_1, \cdots, u_n$ 线性无关. 又因 $\dim V = n+1$, 故 $\{u_0, u_1, \cdots, u_n\}$ 为 V 的一组基. 设 $\Sigma' = \{P_0', P_1', \cdots, P_n'\}$ 为 $\mathcal{P}$ 的另一框架, 并令 u_i' 为 P_i' 之代表元, 则 $\{u_i' | 0 \leq i \leq n\}$ 为 V 的又一组基. 从而有 $\sigma \in GL(V)$, 使得 $u_i^\sigma = u_i'$, $0 \leq i \leq n$. 显然 σ 把 V 的一个子空间映到另一个子空间, 且对 V 的任意二个子空间 $U \subseteq W$, 总成立 $U^\sigma \subseteq W^\sigma$. 由以上讨论可知 σ 导出 $\mathcal{P}$ 到自身的一个映射, 它把 $\mathcal{P}$ 的子空间 α 映到子空间 α^σ, 且由 $\alpha \subseteq \beta$ 可推知 $\alpha^\sigma \subseteq \beta^\sigma$. 由以上讨论可知, $GL(V)$ 中任意元导出射影空间 $\mathcal{P}$ 的自同构. 这表明 $GL(V)$ 作用在 $\mathcal{P}$ 上, 且在 $\mathcal{P}$ 的框架集合上传递.

一般地, $\mathcal{P}$ 中点的一个置换 σ 说是 $\mathcal{P}$ 的一个**共线变换**, 若 σ 把 $\mathcal{P}$ 的子空间映到 $\mathcal{P}$ 的子空间, 且对于 $\mathcal{P}$ 的任意两个子空间 α, β, 总成立: $\alpha \subseteq \beta \Leftrightarrow \alpha^\sigma \subseteq \beta^\sigma$.

现在我们定义 $\mathcal{P}$ 的**射影变换**. 设 $(u_0, u_1, \cdots, u_n)$ 为 V 中一组基, 对于 $v = a_0u_0 + a_1u_1 + \cdots + a_nu_n$, 即 v 在基 $(u_0, u_1, \cdots, u_n)$ 之下具有坐标 $X = (a_0, a_1, \cdots, a_n)$, 我们以 $P(X)$ 表示 $\mathcal{P}$ 中的点 $\langle v \rangle$. $\mathcal{P}$ 上的置换 τ 说是 $\mathcal{P}$ 上一个射影变换, 若可找到矩阵 $\mathrm{Mat}(\tau)$, 使 $\langle v \rangle^\tau = P(X\mathrm{Mat}(\tau))$.

射影变换具有如下性质: 设 $\Lambda = \{P_0, P_1, \cdots, P_n\}$ 和 $\Lambda = \{P_0', P_1', \cdots, P_n'\}$ 是 $\mathcal{P}$ 的两个框架, 则 $\mathcal{P}$ 上有唯一的射影变换 τ, 使 $P_i^\tau = P_i'$.

利用域的自同构 θ, 我们还可以定义 $\mathcal{P}$ 的**共线变换**如下: 令 $X = (a_0, a_1, \cdots, a_n)$ 为 V 中向量 v 的坐标. 记 $X^\theta = (a_0^\theta, a_1^\theta, \cdots, a_n^\theta)$, 则称映射 $P(X) \to P(X^\theta)$ 为 $\mathcal{P}$ 上的共线变换. 作为练习, 请读者自行证明, 任意共线变换都可以写成一个射影变换和一个域自同构所导出的共线变换之积.

命题 3.3 $\mathcal{P}$ 上全体共线变换构成一个群，记作 $P\Gamma L(n,\mathbf{F})$; $\mathcal{P}$ 上全体射影变换也构成一个群，这个群与由 $GL(n,\mathbf{F})$ 中全体元素导出的 $\mathcal{P}$ 上共线变换集合所构成的 $P\Gamma L(n,\mathbf{F})$ 的子群 $PGL(n,\mathbf{F})$ 相重合. 由 $SL(n,\mathbf{F})$ 中全体元素导出的共线变换集合也构成 $P\Gamma L(n,\mathbf{F})$ 的一个子群 $PSL(n,\mathbf{F})$.

我们有下列命题

命题 3.4 一般射影线性群 $PGL(n,\mathbf{F})$ 在 $\mathcal{P}$ 的由 n 个元所构成的无关元组的集合 Ω 上传递. 又群 $PGL(n,\mathbf{F})\cong PGL(V)$, $PSL(n,\mathbf{F})\cong PSL(V)$. 作为 $\mathcal{P}$ 的置换群，$PSL(V)$ 在 $\mathcal{P}$ 上 2 重传递 (关于多重传递置换群的概念，参看第 XII 章 §3).

证 第一个结论可由线性代数有关定理直接得出.

要证明 $PGL(n,\mathbf{F})\cong PGL(V)$, 仅需证若 $\gamma\in G=PGL(V)$, 则 γ 在 $\mathcal{P}$ 上平凡作用，当且仅当 $\gamma\in Z(GL(n,\mathbf{F}))$. 任取 V 中两个无关向量 u,v. 由假定 $u^\gamma=a_uu$, $v^\gamma=a_vv$, $(v+v)^\gamma=a_{u+v}(u+v)$, 其中 $a_u,a_v,a_{u+v}\in\mathbf{F}^\#$. 由于 u,v 线性无关，即得 $a_u=a_v=a_{u+v}$. 这表明，在任意基之下 $\mathrm{Mat}(\gamma)=\mathrm{diag}\{a,a,\cdots,a\}$, $a\in\mathbf{F}^\#$. 这就证明了 $\gamma\in Z(GL(n,\mathbf{F}))$. 反之若 $\gamma\in Z(GL(n,\mathbf{F}))$, 显然 γ 在 $\mathcal{P}$ 上平凡作用.

设 $\{\langle u\rangle,\langle v\rangle\}$ 和 $\{\langle s\rangle,\langle w\rangle\}$ 为 P 中点的二元组. 由于 u 与 v 无关，从而存在 $g\in GL(V)$ 使 $u^g=s$, $v^g=w$, $a=\det g$, $h=a^{-1}g$, $u^h=s$, $v^h=w$. 特别地，$\langle u\rangle^h=\langle s\rangle$, $\langle v\rangle^h=\langle w\rangle$. 这就证明了 $PSL(V)$ 在 $\mathcal{P}$ 上二重传递. □

关于其它典型群有类似的结论. 特别地 $Sp(2n,\mathbf{F})$, $SU(n,\mathbf{F})$, $\Omega(n,\mathbf{F})$, 分别在相应的射影空间上导出射影典型群 $PSp(2n,\mathbf{F})$, $PSU(n,\mathbf{F})$ 和 $P\Omega(n,\mathbf{F})$. 我们将证明，这些射影群，除个别例外，都在各自所属的射影空间的二次锥面 $\mathcal{PC}$ 是本原作用的 (关于本原群和非本原群的概念，参看第 XII 章定义 2.2), 并由此证明，它们都是单的. 在讨论一般情况之前，我们先介绍几个低维射影典型群的性质.

命题 3.5 $PSO(3,q)$ 在 $\mathcal{E}=PG(2,q)$ 中的二次锥面 $\mathcal{EC}$ 上的作用是精确三重传递的，它和 $PGL(2,q)$ 在 $\mathcal{L}=PG(1,q)$ 上的作用相似. 特别地， $PSO(3,q)\cong PGL(2,q)$.

证 设 V 为 $\mathbf{F}=GF(q)$ 上 3 维正交空间. 记 $\mathcal{E}=PG(2,q)$, $\mathcal{E}$ 中二次锥面记作 $\mathcal{EC}$. 由命题 2.6, V 中有双曲对 $\{v_1,v_2\}$, 且 $V=\langle v_1,v_2\rangle\perp\langle v_3\rangle$, 其中 $\langle v_3,v_3\rangle=a\neq 0$.

设 $\langle v\rangle\in\mathcal{EC}$, $v=x_1v_1+x_2v_2+x_3v_3$, 则有 $0=(v,v)=2x_1x_2+ax_3^2$. 若 $x_1=0$, 则 $x_3=0$, 从而 $\langle v\rangle$ 在 $\mathcal{E}$ 上的齐次坐标为 $(0,1,0)$; 若 $x_1\neq 0$, 在 $\langle v\rangle$ 的齐次坐标中可令 $x_1=1$, 从而得 $x_2=-\frac{a}{2}x_3^2$. 由此可知

$$\mathcal{EC}=\{(0,1,0),\ (1,-\frac{a}{2}t^2,\ t)\ \big|\ t\in\mathbf{F}\}.$$

设 $g\in SO(V)$, 且 $(\langle v_2\rangle)^g=\langle v_2\rangle$, 则 g 保持 $\langle v_2\rangle^\perp=\langle v_2,v_3\rangle$ 不变. 从而有 $v_1^g=a_{11}v_1+a_{12}v_2+a_{13}v_3$, $v_2^g=a_{22}v_2$, $v_3^g=a_{32}v_2+a_{33}v_3$, $a_{ij}\in\mathbf{F}$.

这样就有: $(v_1^g,v_1^g)=2a_{11}a_{12}+a_{13}^2=0$, $(v_1^g,v_2^g)=a_{11}a_{22}=1$, $(v_1^g,v_3^g)=a_{11}a_{32}+a_{13}a_{33}=0$. 我们还有 $\det g=a_{11}a_{22}a_{33}=a_{33}=1$. 记 $a_{11}=x$, $a_{13}=y$, 则有

$$g=g(x,y)=\begin{pmatrix} x & \frac{-y^2}{2x} & y\\ 0 & x^{-1} & 0\\ 0 & \frac{-y}{x} & 1\end{pmatrix}.$$

这时 g 导出 $\mathcal{EC}$ 上一个置换 $\overline{g}=\overline{g}(x,y)$.

记 $\overline{H}=\overline{G}_{\langle v_2\rangle}$, 则由 g 的矩阵表达式可知 $|\overline{H}|=q(q-1)$. 且有 $(1,-\frac{a}{2}t^2,t)^{\overline{g}(x,y)}=(x,*,y+t)=(1,*,x^{-1}(y+t))$, 注意，上式及下文中，标准形式的齐次坐标中的 “*” 由其中第三分量唯一确定.

由上式可知, 适当选择 x,y 即可把 $\mathcal{EC}\backslash\{\langle v_2\rangle\}$ 中给定点对变到 $\mathcal{EC}\backslash\{\langle v_2\rangle\}$ 中任意点对. 又若 $\overline{g}=\overline{g}(x,y)\in\overline{H}$, 且 $\overline{g}$ 固定 $\mathcal{EC}\backslash\{\langle v_2\rangle\}$ 中两个点 $(1,-\frac{a}{2}t_1^2,t_1)$ 和 $(1,-\frac{a}{2}t_2^2,t_2)$, 则必有 $x=1$, $y=0$, 即 $\overline{g}=1$. 这表明 $\overline{H}$ 在 $\mathcal{EC}/\{\langle v_2\rangle\}$ 上精确二重传递. 要证明 $\overline{G}$ 在 $\mathcal{EC}$ 上三重传递，仅需证 $\overline{G}$ 在 $\mathcal{EC}$ 上传递即可. 为此令 $s\in G$, $v_1^s=v_2$, $v_2^s=v_1$, $v_3^s=-v_3$, 则有 $(0,1,0)^s=(1,0,0)$, 这就完成了证明.

由以上讨论可知，$\overline{H}$ 为 $\overline{G}$ 之极大子群，特别地 $\overline{G}=\langle\overline{H},\overline{s}\rangle$.

现在我们证明 $\overline{G}$ 在 $\mathcal{EC}$ 上的作用相似于 $PGL(2,q)$ 在射影直线 $\mathcal{L}=PG(1,q)$ 上的作用.

作 $\mathcal{EC}$ 到射影直线 $\mathcal{L}$ 上的映射 $\varepsilon:(0,1,0)^\varepsilon=(0,1),(1,-\frac{a}{2}t^2,t)^\varepsilon=(1,t)$. 规定：$x^\varepsilon\overline{g}=(x\overline{g})^\varepsilon, \forall x\in\mathcal{EC}$. 这样 $\overline{G}$ 忠实作用在 L 上，其中 $(1,t)^{\overline{g}(x,y)}=(1,*,x^{-1}(y+t))^\varepsilon=(1,x^{-1}(y+t))$, $(0,1)^{\overline{s}}=(1,0)$.

又由于 $|\overline{G}|=(q^2-1)q=|PGL(2,q)|$, 即可知，$\overline{G}$ 在 L 上的作用相似于 $PGL(2,q)$ 在 L 上的作用. □

类似地我们可证明如下关于 3 维射影酉群的性质.

命题 3.6 *$PSU(3,q)$ 在 $\mathcal{E}=PG(2,q^2)$ 中的二次锥面 $\mathcal{EC}$ 上的作用是二重传递的.*

注意，一般的特殊射影典型群与同型的低维特殊射影典型群特殊典型群在相应的射影空间或二次锥面上作用的重数有所区别. 除以上两个命题外，定理 2.25 和定理 2.24 表明 1 维射影辛群及 1 维特殊射影酉群在相应的 $\mathcal{LC}$ 上是二重传递的. Parker 证明了，$PSp(4,3)$ 不具有二重传递置换表示. 由于 $PSU(4,2)\cong PSp(4,3)\cong P\Omega(5,3)$, 故 $PSU(4,2)$ 和 $P\Omega(5,3)$ 都不具有二重传递置换表示.

命题 3.7 *(1) 设 $G=SU(V,f)$, $Sp(V,f)$ 或 $O(V,Q)$. 对于任意的 $\gamma\in Z(G)$, 若 $G=Sp(V,f)$ 或 $O(V,Q)$, 则 $\gamma=1$ 或 -1; 若 $G=SU(V,f)$, 则 $\mathrm{Mat}(\gamma)=\mathrm{diag}\{a,a,\cdots,a\}$, $a\in\mathbf{F}^{\#}$, $o(a)\mid(q+1,n)$.*

(2) 设 $G=SU(V,f)$, $Sp(V,f)$ 或 $O(V,Q)$, 则 $\gamma\in G$ 在 $\mathcal{PC}$ 上平凡作用，当且仅当 $\gamma\in Z(G)$.

证 (1) 令 $\gamma\in Z(G)$, 若 $G=Sp(V)$ 或 $SU(V)$, 设 t_u 为以迷向点 $\langle u\rangle$ 为中心的平延；若 $G=O(V,Q)$, 则用 t_u 表示以非迷向点 $\langle u\rangle$ 为中心的反射. 首先假定 t_u 为平延，则 $C_V(t_u)=u^\perp$. $\forall x\in u^\perp$, $(x^\gamma)^{t_u}=(x^{t_u})^\gamma=x^\gamma$, 这表明 $(u^\perp)^\gamma=u^\perp$. 由于 γ 为等距变换，故 $\langle u\rangle^\gamma=\langle u\rangle$, 即 $\forall x\in\langle u\rangle$, 有 $x^\gamma=a_ux$, $a_u\in\mathbf{F}$. 设 $v\in\mathcal{C}$, 则由以上讨论可知，存在 $a_v\in\mathbf{F}$, 使 $v^\gamma=a_vv$. 由 Witt 引理可知，G 在 $\mathcal{PC}$

上传递, 特别地有 $\xi \in G, u^{\xi} = bv, a_v(bv) = (u^{\xi})^{\gamma} = (u^{\gamma})^{\xi} = a_u(bv)$, $a_v = a_u$. 这就证明了, 必然存在 $a \in \mathbf{F}$, 使 $u^{\gamma} = au, \forall u \in \mathcal{C}$. 设 $\{u, v\}$ 为 V 中双曲对, 则有 $1 = (u, v) = (u^{\gamma}, v^{\gamma}) = aa^{\tau}$. 从而可知: $a = \pm 1$, 若 G 为辛群; $o(a) = (q+1, n)$, 若 V 为酉群.

现假定 G 为正交群. 设 $u \in V$, 能使 $(u, u) = 1$. 则 $x^{t_u} = -x$, 当且仅当 $x \in \langle u \rangle$. 由于 $(u^{\gamma})^{t_u} = (u^{t_u})^{\gamma} = -u^{\gamma}$, 则 $\varepsilon_u \in \mathbf{F}$, $u^{\gamma} = \varepsilon_u u$. 由于 γ 为等距, 故有 $\varepsilon_u = \pm 1$. 令 $(u_1, u_2, \cdots, u_n)$ 为 V 的一组正交基, 则有 $u_i^{\gamma} = \varepsilon_i u_i$, $\varepsilon_i = \pm 1$. 令 $i \neq j$, $u_i + u_j$ 非迷向, 则有 $(u_i + u_j)^{\gamma} = \varepsilon(u_i + u_j) = \varepsilon_i u_i + \varepsilon_j u_j$. 由此得 $\varepsilon_i = \varepsilon_j$. 若 $u_i + u_j$ 迷向, 考虑向量 $u = u_j + u_j + u_k$, $k \neq i, j$, 则类似 $u_i + u_j$ 非迷向的情况可得 $\varepsilon_i = \varepsilon_j = \varepsilon_k$. 这就证明了 $\gamma = \pm 1$.

(2) 若 V 为辛群或酉群, 则 (1) 的证明过程同样适用于 (2), 故假定 G 为正交群. 令 $\{u, v\}$ 为 G 中双曲对并取 $z \in \langle u, v \rangle^{\perp}$, 则 z 与 u, v 无关. 令 $x = z - Q(z)u + v$, 则 $Q(x) = Q(z) - Q(z)(u, v) = 0$, 即 x 为迷向的. 设 η 在 $\mathcal{PC}$ 上平凡作用, 则有 $x^{\eta} = c_x x$, $u^{\eta} = c_u u$, $v^{\eta} = c_v v$, 其中 c_x, c_u, $c_v \in \mathbf{F}^{\#}$. 从而有

$$c_x(z - Q(u)u + v) = x^{\eta} = z^{\eta} - c_u Q(u)u + c_v v.$$

由 z 的选取, 得 $z^{\eta} = c_x z$, 从而有 $c_x = c_u = c_v$. 这就证明了 $\eta = cI$, 这里 $c = c_x$, I 为单位阵. 又因 η 正交, 故 $c = \pm 1$. □

引理 3.8 设 $G = Sp(V, f)$, $SU(V, f)$ 或 $\Omega(V, Q)$, 则 G 在 $\mathcal{PC}$ 上且在 $\mathcal{PC}$ 中有序双曲对集合上传递.

证 若 G 为辛群, 则由 Witt 引理立知, G 在 $\mathcal{PC}$ 上且在 $\mathcal{PC}$ 中有序双曲对集合上传递.

现假定 G 为酉群或正交群. 首先证明 G 在 $\mathcal{PC}$ 上的传递性. 设 $\langle u \rangle \neq \langle v \rangle$, $\langle u \rangle, \langle v \rangle \in \mathcal{PC}$. 我们证明, 存在 $\langle z \rangle \in \mathcal{PC}$ 能使 $\{\langle z \rangle, \langle u \rangle\}$, $\{\langle z \rangle, \langle v \rangle\}$ 均为双曲对. 我们先考察情况 $(u, v) = 0$. 这时 $\langle u, v \rangle$ 为一全迷向子空间. 由推论 2.7, 可找到 $s, t \in \mathcal{C}$, 使 $\{u, s\}$, $\{v, t\}$ 均为双曲对, 且 $\langle u, s \rangle \perp \langle v, t \rangle$. 令 $z = s + t$ 即可. 现假定 $\{u, v\}$ 为 V 中双曲对. 若 G 为酉群且 $\operatorname{char} \mathbf{F} = 2$, 则令 $z = u + v$, 易验证 z

合乎要求. 若 char $\mathbf{F}\neq 2$, $G=SU(V)$ 或 $\Omega(V)$, 令 w 为 $\langle u,v\rangle^{\perp}$ 中非迷向向量, $z=u-\frac{(w,w)}{2}v+w$, 则 $Q(z)=0$, $(z,u)\neq 0$ 且 $(z,v)=1$. 故 z 合乎要求.

假定 $\{\langle z\rangle,\langle u\rangle\}$ 和 $\{\langle z\rangle,\langle v\rangle\}$ 均为 $\mathcal{P}$ 中双曲对. 我们证明, 存在 $\eta\in G$ 能使 $\langle z\rangle^{\eta}=\langle z\rangle$, $\langle u\rangle^{\eta}=\langle v\rangle$. 若 G 正交, 这是命题 2.22 的直接结果. 故假定 G 为酉群. 若 $v\in\langle z,u\rangle$, 则有平延 r_u, 能使 $(\langle u\rangle)^{r_u}=\langle v\rangle$. 令 $W=\langle z,u,v\rangle$, 若 $\dim W=2$, 则易见结论成立. 故不妨设 $\dim W=3$ 且 char $\mathbf{F}\neq 2$. 首先设 W 非奇异. 我们以 $\mathcal{PW}$ 表示 W 所对应的射影子空间, 则由命题 3.6, $SU(W)$ 在 $\mathcal{PW}\cap\mathcal{PC}$ 上二重传递. 特别地, 可找到 $\eta\in G$ 使 $\eta|_{W^{\perp}}=1$, $\langle z\rangle^{\eta}=\langle z\rangle$, $\langle u\rangle^{\eta}=\langle v\rangle$. 现假定 W 奇异, 则有 $r\in R(W)$ 使 $v=az+u+r$, $a+a^{\tau}=0$. 故有 $t\in W^{\perp}$, $\{r,t\}$ 为双曲对. 令 $T=\langle z,u,r,t\rangle$. 取 $\eta\in GL(V)$, 使 $z^{\eta}=z$, $u^{\eta}=az+u+r$, $r^{\eta}=z+er-t$, $t^{\eta}=-r$, $\eta|_{T^{\perp}}=1$. 显然 η 即为所求的酉变换.

上述结果表明, G 在 $\mathcal{PC}$ 上传递. 现在我们可以很容易证明, G 在 $\mathcal{P}$ 中双曲对集合上传递. 设 $\{\langle v\rangle,\langle u\rangle\}$ 和 $\{\langle z\rangle,\langle w\rangle\}$ 为 $\mathcal{P}$ 中两个双曲对, 则由 G 在 $\mathcal{PC}$ 上的传递性, 存在 $\eta\in G$, 使 $(\langle v\rangle)^{\eta}=\langle z\rangle$. 又由上述讨论, 可找到 $\zeta\in G$, 使 $(\langle z\rangle)^{\zeta}=\langle z\rangle$, $(\langle u\rangle)^{\zeta}=\langle w\rangle$, 这就证明了 G 在 $\mathcal{P}$ 中有序双曲对集合上传递. □

定理 3.9 *设 $\mathbf{F}=GF(q)$, V 为 $\mathbf{F}$ 上 n 维度量空间. 令: $n=2m$, 若 V 为辛空间; $q=r^2$, 若 V 为酉空间; q 为奇, 若 V 为正交空间. $G=SO(V,f)$ $(\Omega(V,Q))$, 则 G 在 $PG(n,q)$ 中的二次锥面 $\mathcal{PC}$ 上本原作用.*

证 首先证明 $\forall\alpha\in\mathcal{PC}$, $U=G_{\alpha}$ 在 $\mathcal{PC}$ 中有 3 个轨道: $\Delta_1=\{\alpha\}$, $\Delta_2=\{\beta\mid\beta\neq\alpha,\beta\perp\alpha\}$, $\Delta_3=\{\delta\mid(\delta,\alpha)$ 为双曲对$\}$.

设 $\beta_1,\beta_2\in\Delta_2$, 则由 Witt 引理, $\exists g\in G$, 使 $\beta_1^g=\beta_2$, $\alpha^g=\alpha$, 即 U 在 Δ_2 上传递. 同法可证 $\exists h\in G$, 使 $\beta_1^h=\beta_2$, $\alpha^h=\alpha$, 即 U 在 Δ_3 上传递. 记 $\Omega_{\alpha}=\Delta_2\cup\{\alpha\}$, $\Omega'_{\alpha}=\Delta_3\cup\{\alpha\}$. 显然 $\mathcal{PC}=\Omega_{\alpha}\cup\Omega'_{\alpha}$, 且 $\Omega_{\alpha}\cap\Omega'_{\alpha}=\{\alpha\}$.

假定 G 在 $\mathcal{PC}$ 上非本原作用. 设 Λ_{α} 是包含 α 的非本原集. 我们先证明对于任意的 $\alpha\in\mathcal{PC}$, 必然有: (1) $\Lambda_{\alpha}=\Omega_{\alpha}$, 或 (2)

$\Lambda_\alpha = \Omega'_\alpha$. 若 $\alpha \neq \beta \in \Omega_\alpha \cap \Lambda_\alpha$, 则由 U 在 Δ_2 上的传递性可知 $\Lambda_\alpha \supseteq \beta^U = \Omega_\alpha - \{\alpha\}$, 故有 $\Lambda_\alpha \supseteq \Omega_\alpha$. 同法可证若有 $\alpha \neq \beta \in \Omega_{\alpha'} \cap \Lambda_\alpha$, 则 $\Lambda_\alpha \supseteq \Omega_{\alpha'}$. 由于 $\mathcal{PC} = \Omega_\alpha \cup \Omega_{\alpha'}$, 故仅有二者之一成立, 由此立得结论. 注意由于 G 在 $\mathcal{PC}$ 中完全非本原系上传递, 故以上结论适用于任一个非本原集. 以下我们证明, 上述两种情况都将导出矛盾.

若 $\Lambda_\alpha = \Omega_\alpha$, $\forall\alpha \in \mathcal{PC}$. 设 $\{\alpha_1, \alpha_2\}$ 为双曲对, 取 $\alpha_3 \in \langle\alpha_1, \alpha_2\rangle^\perp \cap \mathcal{PC}$. 由定义 $\alpha_1, \alpha_2 \in \Omega_{\alpha_3}$. 由于 $\Lambda_{\alpha_i} = \Omega_{\alpha_i}$, 故有 $\Omega_{\alpha_1} = \Omega_{\alpha_3} = \Omega_{\alpha_2}$, 但显然 $\alpha_1 \notin \Omega_{\alpha_2}$, 矛盾.

现假定 $\Lambda_\alpha = \Omega'_\alpha, \forall\alpha \in \mathcal{PC}$. 选择 $\alpha_1, \alpha_2, \alpha_3$ 如前. 设 $\alpha_i = \langle x_i\rangle$, $i = 1, 2, 3$. 不失一般性可假定 $(x_1, x_2) = 1$. 令 $y = x_1 + x_2$, $\beta = \langle y\rangle$, 则由 $\alpha \in \Lambda_\alpha = \Omega'_\alpha$, 得 $\beta \notin \Omega_{\alpha_2}$ 且 $\beta \in \Omega_{\alpha_3}$, 即得矛盾. □

命题 3.10 *设群 G 作用在集合 S 上, K 为作用核. 则 G/K 为单, 若 G 满足下列条件:*

(1) G 本原地作用在 S 上.

(2) $G = G'$.

(3) 存在 $x \in S$, Stab x 中包含可换正规子群 A_x, 能使 $G = \langle A_x^g \mid g \in G\rangle$.

证 假定有 $H \trianglelefteq G$, 且 H 真包含 K. 则由于 G 在 S 上本原作用, 故 H 在 S 上传递. 令 $G^* = HA_x, x \in S$. 显然 $G^* \lhd G$, 从而 G^* 包含 A_x 在 G 中一切共轭. 由条件 (3), $G = G^* = HA_x$. 故 $G/H \cong A_x/(H \cap A_x)$ 可换. 这表明 $H \geq G' = G$. 故有 $H = G$. 这就证明了 G 为单群. □

定理 3.11 *除掉下文中所列举的例外情况, $PSL(n,q), n \geq 2$; $PSp(2m,q)$, $m \geq 2$; $PSU(n,q)$, $n \geq 2$; $P\Omega(2m+1,q)$, q 为奇, $m \geq 2$; 以及 $P\Omega_{\pm 1}(2m,q)$, q 为奇, $m \geq 3$, 都是单群. 例外情况是: $PSL(2,r) \cong PSU(2,r) \cong PSp(2,r)$, $r = 2$ 或 3; $PSp(4,2)$; $PSU(3,2)$.*

证 我们仅需证明, G 满足命题 3.10 中条件. 由定理 1.4, 2.16, 2.17, 2.23 可知 $G' = G$. 若 $G = PSL(n,q)$, 令 $\Gamma = V^\#$; 在其

它情况下，令 $\Gamma = \mathcal{PC}$. 由命题 3.9 知，G 在 Γ 上作用本原. 现在证明命题 3.10 中条件 (3) 成立. 当 $G = PSL(n,q)$ 时，令 A_x 表示命题 1.3(2) 中的 R_x; 若 $G = \Omega(n,q)$, 令 A_x 等于命题 2.21 中的 H_x; 在其它情况下，令 A_x 等于 $\mathcal{PC}$ 中某一点的根群. 则 G 满足命题 3.10 中之条件. 这就证明了 G 为单群. □

关于偶特征域上的正交群，也有类似结果.

通过以上讨论，我们看到，对于适当的 n, q, 我们可以得到一些典型单群系列. 但当 $n \leq 6$ 时，其中某些群互相同构，或同构于某些置换群. 以下我们列举有关的部分结果 (我们不再重复前文中讨论过的情况): $PSL(2,9) \cong A_6$; $PSL(4,2) \cong A_8$; $PSL(2,7) \cong PSL(3,2)$; $P\Omega(3,q) \cong PGL(2,q)$; $P\Omega(5,q) \cong PSp(4,q)$; $P\Omega_{+1}(4,q) \cong PSL(2,q) \times PSL(2,q)$; $P\Omega_{-1}(4,q) \cong PSL(2,q^2)$; $P\Omega_{+1}(6,q) \cong PSL(4,q)$; $P\Omega_{+1}(6,q) \cong PSU(4,q)$.

注意: 由以上同构关系可得下列诸群非单: $P\Omega(3,q)$, $P\Omega(5,2)$, $P\Omega_{+1}(4,q)$.

利用射影几何，人们定义了各种各样的几何或组合结构，例如以下我们介绍的两种几何和第 XIII 章将要介绍的 Tits 几何，以及设计等. 这些组合结构在理论和实际应用上都十分重要.

配极几何 (polar geometry): 假定 (V,f), (V,Q) 的 Witt 指数 m 为正. (V,f) 或 (V,Q) 的配极几何 Γ 为集合 $I = \{1,2,\cdots,m-1\}$ 上的几何，其中 i 型对象为 V 中射影维数为 i 的全奇异子空间，两个对象 U 和 W 说是关联的，若 $U \subseteq W$ 或 $W \subseteq U$. V 上的等距群 $O(V,f)$ 和相似群 $\Delta(V,f)$ 均作用在 Γ 上.

类旗几何 (oriflamme geometry): 假定 (V,Q) 为一双曲正交空间，且 $\dim V \geq 6$. V 上类旗几何 Γ 为集合 $I = \{1,2,\cdots,m-1\}$ 上的几何，其中型为 i 的对象为射影维数为 $i < m-2$ 的全奇异子空间; 型为 $m-2$ 和 $m-1$ 的对象分别构成 Γ 中如下定义的两个等价类: 令 Λ 为 V 中极大全奇异子空间集合，在 Λ 上定义一个等价关系 $\sim$: $U, W \in \Lambda$, $U \sim W$ 若 $\dim (U/U \cap W)$ 为偶. 则 $\sim$ 为 Λ 上一个等价关系，且 Λ 中恰有两个关于 $\sim$ 的等价类.

$U, W \in \Gamma$ 说是关联的，若 $U \subseteq W$ 或 $W \subseteq U$, 且 $\dim U < m-2$, $\dim W < m-2$. 型为 $m-1$ 和 $m-2$ 的两个对象说是关联的，若 $U \cap W$ 为 U 和 W 的超平面. $\Delta(V,Q)$ 中保持关系 $\sim$ 且在 $\Delta(V,Q)$ 中指数为 2 的子群为 Γ 的自同构群.

§4. $PSL(2,q)$ 的子群结构

1901 年 Dickson 在下列书中给出了 $PSL(2,p^n)$ 的全部子群. 本节中我们将给出 Dickson 定理的部分证明，这些证明综合运用了我们以前所学的基本群论知识，还提供了一些新的处理群论问题的方法.

L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leibzig, Tuebner, 1901. (New York: Dover Publ. 1958.)

设 V 为 $\mathbf{F}=GF(q), q=p^n$, 上 2 维向量空间, $\mathcal{L}$ 为 V 所对应的射影直线. 以齐次坐标表示 $\mathcal{L}$ 中的点, 则 $\mathcal{L}=\{(a,1),(1,0) \mid a \in \mathbf{F}\}$. 通常，我们以 a 表示点 $(a,1)$, 以 ∞ 表示点 (1,0). 按照上述记法，我们可以认为 $\mathcal{L}$ 等同于集合 $\mathbf{F} \cup \{\infty\}$. 我们以 H 表 V 上特殊线性群 $SL(V)$, G 表示 $\mathcal{L}$ 上特殊射影群 $PSL(2,q)$.

以下命题是显然的.

命题 4.1 令 $\mathcal{L}=\mathbf{F}\cup\{\infty\}=\{a,\infty \mid a\in\mathbf{F}\}$, 则 G 由具有如下形状的线性分式映射组成:

$$x \mapsto \frac{ax+b}{cx+d}, \text{其中} a,b,c,d \in GF(q), ad-bc=1.$$

且有:

(1) G 在 $\mathcal{L}$ 的点集合上 2 重传递作用，G 中任意非单位元在 $\mathcal{L}$ 上至多有两个不动点.

(2) $G \cong H/Z(H)$, $H=SL(2,q)$, 其中 $Z(H)\cong Z_2$ 若 $p\neq 2$; $Z(H)=1$ 若 $p=2$. 从而 $|G|=(q+1)q(q-1)/k, k=(q-1,2)$.

命题 4.2 设 P 为 G 的 Sylow p-子群. 则

(1) P 同构于 $\mathbf{F}$ 的加群，特别地，P 为初等可换 p-群. P 中所有的元在 $\mathcal{L}$ 上有一个共同的不动点. 这个点是 P 中任意非单位元唯一的不动点.

(2) $N_G(P) = DP$, 其中 $D = \{g \mid x^g = a^2x, a \in \mathbf{F}^{\#}\}$. D 为循环群，且 D 中每个非单位元恰固定 $\mathcal{L}$ 上两个点： 0 和 ∞, 又 $d = |D| = (q-1)/k, k = (q-1, 2)$, 特别地， $|\mathrm{Syl}_p(G)| = q+1$.

(3) G 中任意两个 Sylow p-子群仅有平凡交. D 与其共轭仅有平凡交.

(4) 设 $Q \leq P$, 则 $N_G(Q) \leq N_G(P)$, 特别地，可找到 $x \in D$ 使 $N_G(Q) = \langle x \rangle P$.

(5) 设 $1 \neq h \in D$, 则 $N_G(\langle h \rangle) = N_G(D)$ 为 $2d$ 阶二面体群.

证 (1) 令 $P = \{g \in G \mid x^g = x + a\}$, 则显然 $P \in \mathrm{Syl}_p(G)$, 且 $P \cong (\mathbf{F}, +)$. 又 ∞ 为 P 中任意非单位元在 $\mathcal{L}$ 上唯一的不动点.

在本命题以下的证明中，我们总假定 P 为 (1) 中所定义的子群.

(2) 由于 ∞ 为 P 在 $\mathcal{L}$ 上唯一的不动点，故也是 $N_G(P)$ 的不动点，特别地

$$N_G(P) \trianglelefteq G_\infty = \{h \mid x^h = a^2x + b, a \in \mathbf{F}^{\#}, b \in \mathbf{F}\}.$$

由 G_∞ 的表达式立知 $P \trianglelefteq G_\infty$. 故 $N_G(P) = G_\infty$. 由此即得，$|\mathrm{Syl}_p(G)| = |G : N_G(P)| = |\mathcal{L}| = q+1$. 其余结论可由定理 1.7(5) 推出.

(3) 设 $P \neq P^g$, 且 $h \in P \cap P^g$, 则 h 固定 ∞ 和 ∞^g. 由 (1), ∞ 为 P 中任意元在 $\mathcal{L}$ 中唯一的不动点，故有 $\infty = \infty^g$. 这就迫使 $P = P^g$, 矛盾.

设 $D \neq D^g$, 且 $h \in D \cap D^g$. 由 (2), h 固定 $0, \infty, 0^h, \infty^h$. 显然， $\{0, \infty\} \neq \{0^h, \infty^h\}$. 这表明 h 至少固定 $\mathcal{L}$ 中 3 个点，从而由命题 4.1, $h = 1$.

(4) 由 (1), 我们可以重复 (2) 的证明过程，并得到 $N_G(Q) \leq N_G(P)$. 显然 $P \leq N_G(Q)$, 故有 $N_G(Q) \leq N_G(Q) \cap PD = (N_G(Q) \cap D)P$, 这表明可找到 $x \in D$, 使 $N_G(Q) = \langle x \rangle P$.

(5) 设 $h\in D, x^h=a^2x, a$ 为 $\mathbf{F}^{\#}$ 中适当的元. 设 $s\in G$ 能使 $x^s=-x^{-1}$. 则成立 $\langle D,s\rangle\le N_G(\langle h\rangle)$. 又 $N_G(\langle h\rangle)$ 必然保持集合 $0,\infty$ 不变, 即 $N_G(\langle h\rangle)$ 中元或固定 0 和 ∞, 或将二者互换, 从而有 $|N_G(\langle h\rangle)|\mid 2|G_{0,\infty}|=2d$. 故成立 $\langle D,s\rangle=N_G(\langle h\rangle)$. 又显然有 $s^2=1$ 且 $h^s=h^{-1}, h\in D$, 这意味着 $N_G(\langle h\rangle)$ 为 $2d$ 阶二面体群. □

命题 4.3 (1) G 中包含 $e=(q+1)/k$ 阶循环群 E.

(2) 若 $1\ne g\in E$, 则 $N_G(\langle g\rangle)$ 为 $2e$ 阶二面体群.

(3) E 的任意两个不相等的共轭有平凡交.

(4) 若 $1\ne g\in E$, 则 g 在 $\mathcal{L}$ 上没有不动点.

证 我们先固定一些符号: $X=SU(2,q), f$ 为乘法群 $GF(q^2)^{\#}$ 的一个生成元, $c=f^{q-1}$.

(1) 由定理 2.24, $SL(2,q)\cong X$. 令

$$y=\begin{pmatrix} c & 0\\ 0 & c^q\end{pmatrix},$$

则 y 为 $SU(2,q)$ 中 $q+1$ 阶元. 以 y_0 记 y 在 $SL(2,q)$ 中的对应元, 则 $o(y_0)=q+1$, 且当 $p\ne 2$, 即 $2\mid q-1$ 时, $\langle y_0^{(q+1)/2}\rangle=Z(H)$. 令 $\bar{y}_0$ 表示 y_0 在射影群 $G=PSL(2,q)$ 中的对应元, 则 $E=\langle\bar{y}_0\rangle$ 为 G 中 $(q+1)/k$ 阶循环群, $k=(q-1,2)$.

(2) 令 $x\in N_X(\langle y\rangle)$. 由于 $y^x\in\langle y\rangle$, 故通过直接计算可知, x 具有以下形状:

$$x=\begin{pmatrix} c^t & 0\\ 0 & c^{tq}\end{pmatrix}\quad 或\quad x=\begin{pmatrix} 0 & c^t\\ c^{tq} & 0\end{pmatrix}.$$

令

$$w=\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}.$$

由以上讨论可知 $N_X(\langle y\rangle)=\langle y,w\rangle$. 显然 $\langle y,w\rangle\cap Z(X)=1$. 这表明 $N_X(\langle y\rangle)$ 在 $PSU(2,q)$ 中的像为 $2e$ 阶二面体群, 这就证明了 $N_G(E)=N_G(\langle y_0\rangle)$ 为 $2e$ 阶二面体群.

(3) 假定 $1 \neq h \in E \cap E^g$. 由 (2) $N_G(E) = N_G(\langle h \rangle) = N_G(E^g)$. 若 $|E| > 2$, 则 E 为二面体群 $N_G(E)$ 中唯一的指数为 2 的循环群. 故有 $E = E^g$. 若 $|E| = 2$, 结论是显然的.

(4) 假定 $h \in E$ 且 h 在 $\mathcal{L}$ 上有一个不动点. 不妨假定该点为 ∞. 则 $o(h)$ 为 $(q+1)/k$ 和 $|N_G(D)| = q(q-1)/k, k = (q-1, 2)$ 的公因子, 这就迫使 $h = 1$. □

命题 4.4 G 中任意元 g 必共轭于 P, D 或 E 中某个元. 确切地说, 若 g 不固定 $\mathcal{L}$ 上任何点, 则 g 必共轭于 $E^{\#}$ 中的元; 若 g 恰固定 $\mathcal{L}$ 中一个点, 则 g 共轭于 $P^{\#}$ 中的元; 若 g 恰固定 $\mathcal{L}$ 中两个点, 则 g 必共轭于 $D^{\#}$ 中的元.

证 由命题 4.2 和命题 4.3, 我们仅需证明:

$$\begin{aligned} & |\bigcup_{g \in G} (P^{\#})^g| + |\bigcup_{g \in G} (D^{\#})^g| + |\bigcup_{g \in G} (E^{\#})^g| + 1 \\ = \ & (q-1)q(q+1)/k = |G|, \quad k = (q-1, 2). \end{aligned}$$

我们有

$$\begin{aligned} & |\bigcup_{g \in G} (P^{\#})^g| + |\bigcup_{g \in G} (D^{\#})^g| + |\bigcup_{g \in G} (E^{\#})^g| + 1 \\ = \ & |G : N_G(P)||P^{\#}| + |G : N_G(D)||D^{\#}| + |G : N_G(E)||E^{\#}| + 1 \\ = \ & 1 + (q+1)(q-1) + \frac{q(q+1)}{2}(\frac{q-1}{k} - 1) + \frac{q(q-1)}{2}(\frac{q+1}{k} - 1) \\ = \ & \frac{(q-1)q(q+1)}{k}. \end{aligned}$$

这就证明了命题 4.4. □

定理 4.5 设 r 为一素数, $R \in \mathrm{Syl}_r(G)$. 则若 $r = p$ 时, R 为初等可换群; 若 $2 \neq r \neq p$ 时, R 为循环群; 而若 $2 = r \neq p$ 时, R 为二面体群.

证 若 $r = p$, 则 R 为 G 中某个 Sylow p-子群, 由命题 4.1(1) 可知, R 为初等可换群. 若 $2 \neq r \neq p$, 由命题 4.2 和 4.3, R 必为循环群 D 或循环群 E 的某个共轭的子群, 故 R 为循环群.

设 $2=r\neq p$. 首先假定 $q\equiv 1(\mathrm{mod}\ 4)$. 则 2 为除尽 $q-1$ 的 2 的最高次幂. 令 2^a 为除尽 $q-1$ 的 2 的最高次幂. 则 $|R|=2^a$. D 中包含 2^{a-1} 阶循环群 B, 从而由命题 4.2 可知, $N_G(B)=N_G(D)$ 中包含 2^a 阶二面体群 R. 显然 $R\in \mathrm{Syl}_2(G)$. 现假定 $q\equiv -1(\mathrm{mod}\ 4)$. 我们可以类似以上讨论证明 $N_G(E)$ 中包含二面体群 $R\in \mathrm{Syl}_2(G)$. □

引理 4.6 设

$$x=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL(2,q).$$

(1) 若 $\mathrm{tr}\ (x)=a+d=\pm 1$, 则有 $x^3=\pm\mathbf{I}_2$.

(2) 若 $\mathrm{tr}\ (x)=0$, 则有 $x^2=-\mathbf{I}_2$.

证 由于 x 在 $GF(q)$ 上的特征多项式次数为 2, 故 x 在 $GF(q^2)$ 中有特征根. 若 ω 为 x 的特征根, 则 ω^{-1} 也是 x 的特征根. 先设 $\mathrm{tr}\ (x)=\omega+\omega^{-1}=-1$. 由此即得 $\omega^{-1}+\omega+1=0$, 故有 $\omega^3=1$. 若 x 的两个特征根 $\omega\neq\omega^{-1}$, 则 x 可表为 $GF(q^2)$ 上对角阵. 这时显然成立 $x^3=1$. 若 $\omega=\omega^{-1}$, 则有 $\omega=1$. 从而有 $\mathrm{tr}\ (x)=2=-1$, 故 $p=3$. 这表明 x 具有形状

$$x=\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

这时又有 $x^3=\mathbf{I}_2$. 若成立 $\mathrm{tr}\ (x)=1$, 则有 $\mathrm{tr}\ (-x)=-1$. 由以上所证, 必有 $x^3=-I_2$.

(2) 由假定,

$$x=\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

其中 $-a^2-bc=1$. 直接计算表明 $x^2=(a^2+bc)\mathbf{I}_2=-\mathbf{I}_2$. □

命题 4.7 $G=PSL(2,q)$ 中包含同构于 A_5 的子群, 当且仅当 $5\mid q(q^2-1)$.

证 若 G 中包含同构于 A_5 的子群，则显然 $5 \mid |G| \mid q(q^2-1)$. 反之，假定 $5 \mid q(q^2-1)$. 若 $5 \mid q$, 即 $p=5$, 则 G 中有子群同构于 $PSL(2,5) \cong A_5$.

若 $p \neq 5$, 则 $5 \mid (q^2-1)$. 假定 $5 \mid q-1$, 则 $GF(q)$ 中有 5 阶元 c. 令

$$x = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}, \quad y = \begin{pmatrix} a & b \\ d & -a \end{pmatrix},$$

其中 $-a^2 - bd = 1$. 由于 $\mathrm{tr}\,(y) = a - a = 0$, 故 $y^2 = -\mathrm{I}_2$. 令 $\bar{y}$ 为 y 在 G 中的对应元. 我们选择 a, 使得 $\mathrm{tr}\,(xy) = a(c - c^{-1}) = 1$. 由等式 $-a^2 - bd = 1$ 确定 b, d, 从而有 $\bar{x}^5 = \bar{y}^2 = (\bar{x}\bar{y})^3 = 1$. 由 I,§6, 习题 3 可知，$\bar{x}, \bar{y}$ 满足 A_5 中生成元之定义关系. 故 $\langle \bar{x}, \bar{y} \rangle$ 为 A_5 的满同态像. 由于 A_5 为单，故有 $\langle \bar{x}, \bar{y} \rangle \cong A_5$.

最后我们假定 $5 \mid q+1$. 取 $a \in GF(q^2), o(a) = 5$.

由于 $q \equiv -1 \pmod 5$, 故 $aa^{\tau} = a^{1+q} = 1$. 注意 $GF(q^2)$ 到 $GF(q)$ 上的范数映射 N 为满射，故可找到 c 使 $N(c) = cc^q = 1 - b^{q+1}$, 其中 $b = (a - a^q)^{-1}$. 令

$$x = \begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix}, \quad y = \begin{pmatrix} b & c \\ -c^q & b^q \end{pmatrix}.$$

显然 $\bar{x}^5 = 1$. 又由 $\mathrm{tr}\,(y) = b + b^q = (a - a^q)^{-1} + (a^q - a)^{-1} = 0$ 及 $\mathrm{tr}\,(xy) = 1$, 得 $\bar{x}^5 = \bar{y}^2 = (\bar{x}\bar{y})^3 = 1$. 仿前一种情况类似可证 $\langle \bar{x}, \bar{y} \rangle \cong A_5$. □

在下文中，我们把同构于 Klein 四元群 ($\cong Z_2 \times Z_2$) 的子群简称为 4-子群.

引理 4.8 设 R 为阶为 $4m$ 的二面体群，则 R 中恰有 2 个 4-子群共轭类. 设 S 为 R 的一个 4-子群，则 $C_R(S) = S$. 且 $N_R(S) = S$, 若 $m \equiv 1 \pmod 2$; $N_R(S) \cong D_8$, 若 $m \equiv 0 \pmod 2$.

证 令 $R = \langle a, b \mid a^{2m} = b^2 = 1, a^b = b^{-1} \rangle \cong D_{4m}^{\cdot}$. 则 R 中 4-子群均具有以下形状

$$\langle a^m, a^i b \rangle, i = 0, 1, \cdots, 2m-1. \tag{$*$}$$

这些子群分为以下两个共轭类:

$$\langle a^m, a^{2j}b\rangle, j=0,1,\cdots,m-1;\quad \langle a^m, a^{2j+1}b\rangle, j=0,1,\cdots,m-1.$$

设 $S=\langle a^m, a^ib\rangle, x\in C_R(S)$. 若 $x=a^j$, 则有 $a^ib=(a^ib)^{a^j}=a^{i-2j}b$. 这表明 $j=m$, 特别地, $x\in S$. 若 $x=a^jb$, 则有 $a^ib=(a^ib)^{a^jb}=a^{2j-i}b$. 从而必有 $2i-2j\equiv 0(\mathrm{mod}\ m)$, 即 $x=a^ib$ 或 $x=a^{i+m}$. 这就证明了 $x\in S$. 基本上依照以上证法, 便可得出关于 $N_R(S)$ 的结论. □

命题 4.9 (1) *G 中包含同构于 S_4 的子群当且仅当 $q^2-1\equiv 0(\mathrm{mod}\ 16)$.*

(2) *G 中包含同构于 A_4 的子群当且仅当 $p\neq 2$ 或 $p=2,n$ 为偶.*

证 (1) 若 G 中包含同构于 S_4 的子群, 则 $24\mid |G|$. 由于 $p\neq 2$, 故 $16\mid (q^2-1)$. 现假定 $16\mid (q^2-1)$. 这时必有 $8\mid q-1$ 或 $8\mid q+1$; 令 $Y=D$, 若 $8\mid q-1$. 令 $Y=E$, 若 $8\mid q+1$. 则 Y 为 $8m$ 阶循环群, 且 $N_G(Y)$ 为 $16m$ 阶二面体群. 令 $\Omega=\{(x,y)\mid x,y\in G,\langle x,y\rangle\cong Z_2\times Z_2\}$. 我们设法计算 Ω, 并由此得出 G 中所包含 4-子群之个数. 我们先计算 G 中 2 阶元个数. 设 x 为 G 中 2 阶元, 则由命题 4.4, 可找到 $g\in G$ 使 $x^g\in Y$, 且 x^g 为 Y 中唯一的 2 阶元. 这表明 G 中恰包含 $k=|G:N_G(Y)|=(q+1)q(q-1)/32m$ 个 2 阶元, 且 G 中仅有一个对合共轭类. 假定 y 为 Y 中唯一的对合. 设 $\langle x,w\rangle$ 为一 4-群. 因 $x^w=x$, 根据引理 4.7 必有 $w\in N_G(Y)$. 注意在 $N_G(Y)$ 中有 $8m$ 个不同于 x 的对合. 这表明 $N_G(Y)$ 中有 $8km=(q+1)q(q-1)/4$ 个对合序对 (x,w). 由于每个 4-群中的元可以构成 G 中 6 个不同的对合序对, 故 G 中包含 $(q+1)q(q-1)/24=|G|/12$ 个 4-群. 设 $W=\langle v,w\rangle$ 为 G 中一个 4-子群. W 必然共轭于 $N_G(Y)$ 中某个 4-子群, $C_G(W)\leq N_G(Y)$. 从而由引理 4.8 可知 $C_G(W)=W$. 这表明 $N_G(W)/W$ 同构于 S_3 的一个子群, 特别地, $|N_G(W)/W|\mid 6$. 由于 $|G|\equiv 0(\mathrm{mod}\ 8)$, 故 W 真包含于 $N_G(W)$ 的某个 Sylow 2-子群之中. 这表明 $|N_G(W)|\equiv 0(\mathrm{mod}\ 8)$.

若 G 中仅包含一个 4-子群共轭类，则 $|G|/12 = |G : N_G(W)|$. 从而有 $|N_G(W)| = 12$, 矛盾. 故 G 中包含两个 4-子群共轭类. 设 W_1 和 W_2 分别为这两个共轭类之代表，并令 $k_i = |N_G(W_i)/W_i|, i = 1, 2$. 我们有 $|G|/12 = |G|/4k_1 + |G|/4k_2$. 因 $k_i \mid 6$, 故必有 $k_1 = k_2 = 6$. 这就证明了 $|N_G(W_i)| = 24$.

最后我们证明 $N_G(W) \cong S_4$. 由以上讨论可知 $N_G(W)/W \cong S_3$. 以 Q 表示 $N_G(W)$ 中一个 Sylow 2-子群，则 Q 为二面体群. 令 $s_1 \in Q\backslash W, s_2 \in N_G(W)\backslash Q$ 均为对合，则 $U = \langle s_1, s_2\rangle$ 为二面体群，且 U 不可能为 2-群. 故 $U \cong S_3$. 由于 $|N_G(W) : U| = 4$, 所以 $N_G(W)$ 同态于 S_4 的一个子群. 显然 $N_G(W)$ 在 U 的陪集集合上作用的核为 1, 故有 $N_G(W) \cong S_4$.

(2) 假定 G 中包含同构于 A_4 的子群. 若 $p = 2$, 则必有 $3 \mid 2^n - 1$. 显然若 $n > 0$, 则仅当 n 为偶时 $3 \mid 2^n - 1$.

现假定 $p = 2$, n 为偶. 则 $G = PSL(2,q)$ 中包含同构于 $PSL(2,4) \cong A_5$ 的子群，当然也包含同构于 A_4 的子群. 若 p 为奇，则由 (1) 的证明可知 $|N_G(W)| \mid 24$, $12 \mid |N_G(W)|$, 且 $C_G(W) = W$. 故 $N_G(W)$ 中包含同构于 A_4 的子群. □

命题 4.10 (1) 若 $m \mid n$, $q = p^n$, 则 $PSL(2,q)$ 中包含同构于 $PSL(2,p^m)$ 的子群.

(2) 若 $2m \mid n$, $q = p^n$, 则 $PSL(2,q)$ 中包含同构于 $PGL(2,p^m)$ 的子群.

证 (1) 由于 $GF(p^m)$ 是 $GF(q)$ 的子域，故 (1) 中结论显然成立.

(2) 由于 $GF(p^m)$ 是 $GF(q)$ 的子域，故有 $PGL(2,p^m) \leq PGL(2,q)$. 要完成证明，我们仅需证，若 $n = rm \equiv 0 \pmod{2m}$, 则 $GF(p^m)^\#$ 中每个元都是 $GF(q)^\#$ 中的平方元. 若 $p = 2$, 这是显然的. 现假定 $p \neq 2$. 这时我们有: $|GF(p^{rm})^\# : GF(p^m)^\#| = (p^{rm} - 1)/(p^m - 1) = 1 + p^m + \cdots + p^{(r-1)m} \equiv r \equiv 0 \pmod 2$. 由此立得 (2) 中的结论. □

命题 4.2 – 命题 4.10 给出了如下定理的部分证明.

定理 4.11 令 $G = PSL(2,q)$, $H \leq G$. 则 H 同构于下列子群之一:

(1) $2(q \pm 1)/k$ 阶二面体群及其子群，其中 $k = (q-1,2)$.

(2) $q(q-1)/k$ 阶群及其子群，H 的 Sylow p-子群 Q 为初等可换群，$Q \trianglelefteq H$, 且商群 H/Q 为 $(q-1)/k$ 阶循环群.

(3) A_4, S_4, 或 A_5.

(4) $PSL(2,p^m)$ 或 $PGL(2,p^m)$, 其中 $m \mid n$.

作为定理 4.11 的推论，我们有如下定理:

定理 4.12 设 $G = PSL(2,q)$. 则 G 中真子群在 G 中的最小指数为 $q+1$, 除非 $q = 2,3,5,7,9$. 在这些例外情况中，最小指数为 q, 若 $q < 9$. 当 $q = 9$ 时，最小指数为 6.

证　注意 G 的所有子群均属于定理 4.11 中所列举的情况之一. 定理 4.11(1) 中子群最大阶数为 $2(q+1)$, 故若 $q > 3$, 则最小指数为 $q(q-1)/2 > q+1$. 定理 4.11(2) 中子群最小指数为 $q+1$. 在定理 4.11(4) 中，令 $n = rm$, 则其中子群的指数至少为 $r^{m-1}(r^{2(m-1)} + \cdots + r^2 + 1)/2 > q+1$. 若定理 4.11(3) 中某个子群在 G 中之指数小于 $q+1$, 则必有 $q(q^2-1)/k < 60(q+1)$, 其中 $k = (2, q-1)$. 这表明 q 的上限为 11. 对于 $q \leq 11$, 我们利用定理 4.11, 考察所有可能的情况，即可得出所需结论：若 $q = 4$ 或 8, 则极小指数为 $q+1$; 其他情况均与定理所述一致. □

要完全地证明定理 4.11, 还须证 H 仅可能同构于定理中所列举的群之一. 限于篇幅，我们略去了有关的证明. 这一证明比较复杂，有兴趣的读者可以在前言中指出的 M. Suzuki 和 B. Huppert 的群论教科书中找到该证明. (在 Suzuki 的书中，作者先讨论了 $SL(2,q)$ 的子群结构，然后作为推论，得出 $PSL(2,q)$ 的子群结构). 他们的证明思路基本相同，都是通过两种方法计算群中元素个数，从而得出子群的可能的类型.

习　题

1. (1) 令 $\mathbf{F}=GF(q^2)$, (V,f) 为 $\mathbf{F}$ 上 3 维酉空间, $G=GU(V)$. 证明 V 中可以找到基 X, 使得如下定义的 P 为 G 的一个 Sylow p-子群.

$$P=\left\{g\;\middle|\;\mathrm{Mat}(g)=\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}\right\}.$$

证明 P' 为 G 中一个根群.

(2) 令 $\mathbf{F}=GF(2)$, (V,f) 为 $\mathbf{F}$ 上 4 维酉空间. 令 $X=\{x_i|1\le i\le 4\}$ 为 V 的一组正交基, $\Delta=\{\langle x_i\rangle \mid x_i\in X\}$. 记 $G=SU(V)$. 我们应用第 XII 章定义 1.2 的符号和术语, 用 $G_{\{\Delta\}}$ 表示 Δ 在 G 中的集型稳定子群, 而用 $G_{(\Delta)}$ 表示 Δ 在 G 中的点型稳定子群. 证明: $G_{\{\Delta\}}/G_{(\Delta)}\cong S_4$, $G_{(\Delta)}$ 和 $G_{\{\Delta\}}$ 由平延生成. 令 $D\in\Delta$, $\Gamma=\{\Delta^h \mid h\in G_D\}$. 证明 $G_D/G_{(\Gamma)}\cong A_4$, 且 $|G_{(\Gamma)}|=54$.

2. 令 $\mathbf{F}$ 为一域, $\theta\in\mathrm{Aut}(\mathbf{F})$, V 为 $\mathbf{F}$ 上 n 维向量空间. 映射 $f:V\times V\to\mathbf{F}$ 说是 V 上关于 θ 的半线性型, 若 $\forall u,v,w\in V,a\in\mathbf{F}$ 成立:

$$f(u+v,w)=f(u,w)+f(v,w),$$

$$f(au,v)=af(u,v),$$

$$f(u,v+w)=f(u,v)+f(u,w),$$

$$f(u,av)=a^{\theta}f(u,v).$$

半线性型 g 说是和 f 相似的, 若 $g=\lambda f$, $\lambda\in\mathbf{F}$. 证明若 f 为 V 上半线性型, 能使下列关系成立:

$$\forall u,v\in V, f(u,v)=0\Longleftrightarrow f(v,u)=0.$$

则下列情况之一成立:

(1) $f(u,u)=0$, $\forall u\in V$, $\theta=1$, 且 f 为斜对称的;

(2) 存在 $u\in V$, 使 $f(u,u)\neq 0$, 且下列之一成立:

(i) $\theta=1$, 且 f 为对称双线性型;

(ii) $o(\theta)=2$ 且 f 相似于一个厄米特型;

(iii) $o(\theta)>2$ 且 $\dim R(V)\ge\dim V-1$, 其中 $R(V)$ 是 V 的根.

3. 设 (V,Q) 为域 $\mathbf{F}$ 上 4 维正交空间, $\nu(V)=2$. 以 $\mathcal{PC}$ 表示 V 中全体迷向点之集合. 证明, $\Omega(V,Q)$ 在 $\mathcal{PC}$ 上非本原作用, 并由此证明 $P\Omega(V,Q)$ 非单.

4. 设 V 为域 $\mathbf{F}$ 上 $2n$ 维线性空间, t 为 $G=Sp(V)$ 中对合. 证明

(1) 若 char $\mathbf{F} \neq 2$, 则 V 有正交分解 $V = V_1 \perp V_2$, 且 $v_1^t = v_1$, $\forall v_1 \in V_1$, $v_2^t = -v_2$, $\forall v_2 \in V_2$.

(2) 若 char $\mathbf{F} = 2$, 则 V 中有 n 维全迷向子空间 W, 能使 $w^t = w$, $\forall w \in W$.

5. 令 $\Delta = \{PSL(2,q), SL(2,q), PSU(3,q), SU(3,q)\}$, $G \in \Delta$, $S \in \mathrm{Syl}_p(G)$, K 为 S 在 $N_G(S)$ 中的补. 则有

(1) G 在集合 $\{N_G(T) \mid T \in \mathrm{Syl}_p(G)\}$ 上作用 2 重传递, 且 $N_G(S)$ 为 G 中极大子群.

(2) K 循环且 $Z(G) \leq K$. 假定 $q > 3$, 若 $G \cong PSL(2,q)$ 或 $SL(2,q)$; $q > 2$, 若 $G \cong PSU(3,q)$ 或 $SU(3,q)$. 则 K 不可约地作用在 $Z(S)$ 和 $S/\Phi(S)$ 上; $C_S(K) = 1$, $|N_G(K) : K| = 2$, $C_G(K) = K$, 且 K 恰正规化两个 Sylow p-子群;

(3) 若 $x \in \mathrm{Aut}(G)$ 为一 p' 元且中心化 S, 则 $x = 1$.

6. 证明:

(1) $|GU(n,q)| = q^{n(n-1)/2}(q+1)\prod_{i=2}^{n}(q^i - (-1)^i)$;

(2) $|O(2m+1,q)| = 2q^{m^2}\prod_{i=1}^{m}(q^{2i} - 1)$.

7. 证明定理 2.25.

8. 证明:

(1) $PSL(2,9) \cong A_6$;

(2) $PSL(4,2) \cong A_8$.

9. 设 $\mathbf{F} = GF(q), q = p^n$, $G = SL(2,q), H = GL(2,q)$. 证明

(1) G 有一个 n 阶外自同构;

(2) G 的任意自同构必然具有以下形状:

$$\sigma : A \mapsto Q^{-1}A^{\alpha}Q, \forall A \in G,$$

其中 $Q \in H, \alpha \in \mathrm{Aut}(\mathbf{F})$. (注意若 $A = (a_{ij})$ 为 $\mathbf{F}$ 上 n 级矩阵, 则 $A^{\alpha} = (a_{ij}^{\alpha})$.)

10. (1) 设 G 为一群, $G' = G$, $G/Z(G) \cong A_5$, 且 $Z(G) \neq 1$, 则有 $G \cong SL(2,5)$, 特别地 $Z(G) \cong Z_2$.

(2) 设 G 为一非可解群, $|G| = 120$. 证明 G 必同构于 S_5, $A_5 \times Z_2$ 或 $SL(2,5)$.

11. 证明 $PSL(2,q)$ 的极大子群必为下列诸群之一:

(1) $2(q-\varepsilon)/d, \varepsilon = \pm 1$ 阶二面体群, 其中 $d = (2, q-1)$; 注意对于下列情况结论不成立: 若 $\varepsilon = 1, q = 3, 5, 7, 9$; 或 $\varepsilon = -1, q = 2, 7, 9$;

(2) $q(q-1)/d$ 阶可解群;

(3) A_4, 若 q 为大于 3 的素数, 且 $q \equiv 3, 13, 27, 37 (\mathrm{mod}\ 40)$;

(4) S_4, 若 q 为素数且 $q \equiv -1 (\mathrm{mod}\ 5)$;

(5) A_5, 其中 q 为下列情况之一: $q = 5^m$ 或 4^m, 其中 m 为素数; q 为素数且同余于 $\pm 1 (\mathrm{mod}\ 5)$; 或 q 为一奇素数的平方, 且 $q \equiv -1 (\mathrm{mod}\ 5)$;

(6) $PSL(2, r)$, 其中 $q = r^m$, m 为一奇素数;

(7) $PGL(2, r)$, 其中 $q = r^2$.

12. 一个非可换单群 G 说是一个 *极小单群*, 若 G 的任何真子群均可解. 证明 $PSL(2, q)$ 为极小单群, 当且仅当 q 属于下列情况之一: $q = 2^m$, m 为素数; $q = 3^s$, s 为奇素数; q 为大于 5 的素数, 且 $q \equiv \pm 2 (\mathrm{mod}\ 5)$; 或 $q = 5$.

第 XII 章

置换群

人们对群的认识从置换群始. 实际上 Galois 在研究多项式的根式可解问题时, 就曾把域 **F** 的自同构看成 **F** 中一组生成元集的置换. 因此置换群论有悠久的历史. 近几十年, 置换群的研究十分活跃, 并且随着有限单群分类工作的完成, 一些重要的问题获得解决. 另一方面, 置换群与组合结构有密切的联系. 这也成为置换群研究的又一动力. 在本章中, 我们较系统地介绍置换群的理论. 本章前三节用来建立置换群的一些重要概念, 后面六节则对某些课题进行讨论. 但限于篇幅, 我们的讨论只能是初步的, 有兴趣的读者可以参看下列的专著或论文.

1) H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

2) J.D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics No. 163; Springer-Verlag, 1996.

3) P.M. Neumann, Finite permutation groups, edge-coloured graphs and matrices, in *Topics in Group Theory and Computation*, (Proc. of a summer school at University College, Galway, 1973); Edited by M. P. J. Curran, Academic Press, 1977. Chap. 5, pp. 82–118.

4) P.J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13**(1981), 1–22.

§1. 置换群的基本概念

设 Ω 是一个非空集合. 称对称群 S_Ω 的子群为 Ω 上的置换群.

在本章中我们只考虑有限置换群, 故下面恒假定 Ω 是有限集合. 有时还假定 $\Omega = \{1, 2, \ldots, n\}$. 以后称 Ω 中元素为点.

设 G 是 Ω 上的置换群, 即 $G \leq S_\Omega$. 对于 $i \in \Omega, g \in G, i$ 在 g 之下的像记作 i^g. 而对于 $\Delta \subseteq \Omega$, 规定

$$\Delta^g = \{\delta^g \mid \delta \in \Delta\}.$$

给定 Ω 上的置换群 G. 我们可在 Ω 上规定一个等价关系 "$\sim$":

$$i \sim j \iff \text{存在 } g \in G \text{ 使 } i^g = j.$$

("$\sim$" 是等价关系请读者自行验证.) 对于关系 "$\sim$" 的等价类叫做 G 在 Ω 上的 *轨道*. 明显地, 如果 $i \in \Omega$, 则

$$i^G = \{i^g \mid g \in G\}$$

是 G 的一个轨道.

定义 1.1 设 $G \leq S_\Omega$. 若 G 在 Ω 上只有一个轨道, 即 Ω 本身, 则称 G 为 Ω 上的 *传递群*, 否则称 G 为 Ω 上的 *非传递群*.

定义 1.2 设 $G \leq S_\Omega, \Delta \subseteq \Omega$. 规定

$$G_{(\Delta)} = \{g \in G \mid \delta^g = \delta,\ \forall \delta \in \Delta\},$$

称为 G 对 Δ 的 *点型稳定子群*. 如果 $\Delta = \{i\}$ 或 $\{i, j\}$, 常记 $G_{(\Delta)}$ 为 G_i, G_{ij} 等等, 有时也记 $G_{(\Delta)}$ 为 G_Δ.

又规定

$$G_{\{\Delta\}} = \{g \in G \mid \Delta^g = \Delta\},$$

称为 G 集合 Δ 的 *集型稳定子群*.

我们有下面的

命题 1.3 $G_{(\Delta)} \trianglelefteq G_{\{\Delta\}}$.

在第 II 章 §1, 关于轨道, 传递性, 稳定子群等概念已证明了下述结果.

命题 1.4 设 $G \le S_\Omega$.

(1) 若 $\Delta \subseteq \Omega$ 是 G 的轨道, $s \in S_\Omega$, 则 Δ^s 是 $s^{-1}Gs$ 的轨道.

(2) 若 $\Delta \subseteq \Omega$, $g \in G$, 则 $g^{-1}G_{(\Delta)}g = G_{(\Delta^g)}$, $g^{-1}G_{\{\Delta\}}g = G_{\{\Delta^g\}}$.

定理 1.5 设 $G \le S_\Omega$, $i \in \Omega$, 则

$$|G_i||i^G| = |G|.$$

(参看第 II 章命题 1.2 和定理 1.5.)

定义 1.6 设 G 为 Ω 上的非传递群, Δ 是 G 的一个轨道, $g \in G$. 以 g^Δ 记 g 在 Δ 上诱导的置换. 令

$$G^\Delta = \{g^\Delta \mid g \in G\}.$$

称 G^Δ 为 G 在 Δ 上的 *传递成分*.

明显的, 映射 $g \mapsto g^\Delta$ 是 G 到 G^Δ 上的同态, 其核为 $G_{(\Delta)}$. 于是我们有 $G^\Delta \cong G/G_{(\Delta)}$. 如果这个同态的核是单位子群, 则称传递成分 G^Δ 是忠实的.

定义 1.7 设 $G \le S_\Omega$, $i \in \Omega$. 称 i 为 G 的 *不动点*, 如果 $i^g = i$, $\forall g \in G$. 这时 $\{i\}$ 是 G 的一个长为 1 的轨道.

我们以 $\mathrm{fix}_\Omega(G)$ 表 G 在 Ω 上全体不动点的集合.

类似地, 对于 $g \in G$, 我们规定 $\langle g\rangle$ 的不动点为 g 的不动点, 并以 $\mathrm{fix}_\Omega(g)$ 表示 g 的全体不动点的集合.

命题 1.8 设 $G \le S_\Omega$ 是传递置换群, $\alpha \in \Omega$, $\Phi = \mathrm{fix}_\Omega(G_\alpha)$, $N = N_G(G_\alpha)$. 则 N 在 Φ 上传递. 特别地, G_α 的不动点的个数为 $|N : G_\alpha|$.

证 设 $n \in N$, $\beta \in \Phi$. 因 $\beta^{nG_\alpha} = \beta^{G_\alpha n} = \beta^n$, 故 $\beta^n \in \Phi$. 于是 Φ 是 N 的不变集.

对任意的 $\beta \in \Phi$, 存在 $g \in G$ 使 $\alpha^g = \beta$. 并且因 $\alpha^{gG_\alpha g^{-1}} = \alpha$, $gG_\alpha g^{-1} \leq G_\alpha$, 有 $g \in N$. 于是 Φ 是 N 的轨道. □

定义 1.9 设 $G \leq S_\Omega$. 称 $|\Omega| - |\mathrm{fix}_{\,\Omega}(G)|$ 为 G 的 *级或次数*. G 的级是被 G 实际变动的文字个数, 记作 $\deg G$.

类似地, 对 $g \in G$, 规定 $\deg g = \deg\langle g\rangle$, 叫做元素 g 的级或次数. 而

$$\min\{\deg g \mid g \in G, g \neq 1\}$$

叫做 G 的 *最小级或最小次数*.

定义 1.10 设 $G \leq S_\Omega$. 若对任意的 $i \in \Omega$, 恒有 $G_i = 1$, 则称 G 为 *半正则的*, 如果半正则群 G 又在 Ω 上传递, 则称 G 为 *正则群*.

显然, G 在 Ω 上半正则 $\Longleftrightarrow$ G 的最小次数为 $|\Omega|$. 又, 抽象群 G 的右正则表示是 G 上的正则置换群.

命题 1.11 *Ω 上半正则群 G 的所有轨道长都是 $|G|$. 由此, Ω 上传递群 G 正则 $\Longleftrightarrow$ $|\Omega| = |G|$.*

证 对任意的 $i \in \Omega$. 由 $|G_i||i^G| = |G|$ 及 $G_i = 1$ 得 $|i^G| = |G|$. □

为证明下列命题, 我们回忆一下, 设 G 是任意群, 对于 $g \in G$, 规定 G 到 G 上的映射

$$R(g) : x \mapsto xg, \ \forall x \in G,$$

和

$$L(g) : x \mapsto g^{-1}x, \ \forall x \in G.$$

则映射 $g \mapsto R(g)$, $\forall g \in G$ 和映射 $g \mapsto L(g)$, $\forall g \in G$ 都是 G 到 S_G 内的同构映射, 分别叫做 G 的右正则表示和左正则表示. 并且 $R(G)$ 在 S_G 中的中心化子恰为 $L(G)$, 即 $C_{S_G}(R(G)) = L(G)$. (同样也有 $C_{S_G}(L(G)) = R(G)$.)

命题 1.12 设 $G \le S_\Omega$, $C = C_{S_\Omega}(G)$. 则 G 半正则 $\Longleftrightarrow$ C 在 Ω 上传递.

证 $\Longleftarrow$: 设 $i, j \in \Omega$. 由 C 传递, 存在 $x \in C$ 使 $i^x = j$. 于是 $G_i = x^{-1}G_ix = G_{i^x} = G_j$. 由 j 的任意性, 得到 $G_i = 1$. 又由 i 的任意性, 得 G 的半正则性.

$\Longrightarrow$: 先设 G 是正则的. 则 G 置换同构于 G 的右正则表示 $R(G)$, 而 $R(G)$ 在 S_G 中的中心化子是 $L(G)$, 即 G 的左正则表示. 由此即得 C 在 Ω 上传递.

再设 G 在 Ω 上有 k 个轨道, $k > 1$. 设其轨道为 $\Omega_1, \cdots, \Omega_k$. 则 G 在每个轨道 Ω_i 上的传递成分是正则的, 并置换同构于 G 的右正则表示. 于是, 若等同 Ω_i 与集合 $\Delta_i = \{x^{(i)} \mid x \in G\}$, 则 G 可看成集合 $\Delta = \bigcup_{i=1}^k \Delta_i$ 上的置换群, 且对任意的 $g \in G$, g 在 Δ 上的作用为 $g : x^{(i)} \mapsto (xg)^{(i)}$, $\forall i$.

现在设 σ 是 $\{1, \cdots, k\}$ 的任一置换, $g \in G$. 定义 Δ 的置换

$$L(\sigma, g) : x^{(i)} \mapsto (g^{-1}x)^{(i^\sigma)}, \ \forall i.$$

则 $L(\sigma, g) \in C_{S_\Delta}(G)$. 因为 $C \ge \{L(\sigma, g) \mid g \in G, \sigma \in S_k\}$, 由此得 C 的传递性. □

命题 1.13 设 $G \le S_\Omega$, G 传递. 令 $C = C_{S_\Omega}(G)$. 则 C 半正则. 但其逆不真.

证 由命题 1.12, 因 $G \le C_{S_\Omega}(C)$ 立得 C 半正则.

反过来, 若 $C = C_{S_\Omega}(G)$ 半正则, G 不一定传递. 例如, 令 $\Omega_1 = \{1, 2, 3\}$, $\Omega_2 = \{4, 5, 6\}$, $\Omega = \Omega_1 \cup \Omega_2$. 令 $G = S_{\Omega_1} \times S_{\Omega_2}$. 则 G 非传递, 但 $C = C_{S_\Omega}(G) = 1$, 当然半正则. □

命题 1.14 设 $G \le S_\Omega$, G 交换, 且在 Ω 上传递, 则 G 正则, 并且 $C_{S_\Omega}(G) = G$.

证 首先, $C = C_{S_\Omega}(G) \ge G$, G 又在 Ω 上传递, 由 1.12, G 半正则, 又由 G 的传递性得 G 正则. 用同样的推理得 C 也在 Ω 上正则, 这样

$$|C| = |\Omega| = |G|.$$

因为 $C \geq G$, 即得 $C = G$. □

§2. 非本原群和本原群

定义 2.1 设 $G \leq S_\Omega, \Delta \subseteq \Omega$. 若对任意的 $g \in G$, 或者 $\Delta^g = \Delta$, 或者 $\Delta^g \cap \Delta = \varnothing$, 则称 Δ 为 G 的一个 *块* (block).

显然, Ω, $\varnothing$ 以及单点子集 $\{i\}$ 都是 G 的块, 它们叫做 *平凡块*.

定义 2.2 设 $G \leq S_\Omega$. 如果 G 存在一个非平凡块 Δ, 则称 G 为 *非本原群*, 此时称 Δ 为 G 的一个 *非本原集*. 当 $|\Omega| = 2$ 时, 我们约定, 当 G 为单位元群时也说 G 为非本原群.

由此定义, 非传递群自然都是非本原群.

定义 2.3 设 $G \leq S_\Omega$, 如果 G 不是非本原群, 则称 G 为 Ω 上 *本原群*.

明显的, 本原群一定是传递群, 在本节剩下的部分, 永远假定 G 是 Ω 上的传递置换群.

命题 2.4 *设 $G \leq S_\Omega$, G 传递但非本原. 并设 Δ 为一非本原集. 令 $H = G_{\{\Delta\}} = \{g \in G \mid \Delta^g = \Delta\}$, 则子群 H 在 Δ 上传递. 设 $G = \bigcup_{r\in R} Hr$ 是 G 对 H 的右陪集分解, 则*

(1) $\Omega = \bigcup_{r\in R} \Delta^r$, *且对 $r \neq r'$ 有 $\Delta^r \cap \Delta^{r'} = \varnothing$;*

(2) $|\Delta| \mid |\Omega|$.

证 对任意的 $i, j \in \Delta$, 由 G 传递, 存在 $g \in G$ 使 $i^g = j$. 这时 $j \in \Delta \cap \Delta^g$, 故 $\Delta \cap \Delta^g \neq \varnothing$. 由 Δ 是块, 得 $\Delta = \Delta^g$, 于是 $g \in H$, 遂得 H 在 Δ 上的传递性.

下面设 $G = \bigcup_{r\in R} Hr$ 是 G 对 H 的右陪集分解.

(1) 设 $i \in \Delta$, $j \in \Omega$. 由 G 之传递性, 有 $g \in G$ 使 $j = i^g \in \Delta^g$. 令 $g = hr$, 其中 $h \in H$, $r \in R$. 于是 $j \in \Delta^{hr} = \Delta^r$, 因此 $\Omega = \bigcup_{r\in R} \Delta^r$.

又若 $\Delta^r \cap \Delta^{r'} \neq \varnothing$, 则 $\Delta^{rr'^{-1}} \cap \Delta \neq \varnothing$. 由 Δ 是非本原集，有 $\Delta = \Delta^{rr'^{-1}}$. 于是 $rr'^{-1} \in H$, $Hr = Hr'$. 由 R 是 H 的陪集的完全代表系，有 $r = r'$.

(2) 由 $|\Delta| = |\Delta^r|$ 和 (1) 立得. □

(1) 中所给出的 $\{\Delta^r \mid r \in R\}$ 称为 G 的 *完全非本原系*. (1) 断言 $\Omega = \bigcup_{r\in R} \Delta^r$ 是一个无交并. 通常我们把 Ω 的这种表成子集无交并的分解称为 Ω 的一个 *分划*. 分划 $\Omega = \Delta_1 \cup \cdots \cup \Delta_k$ 称为平凡的，若 $k = 1$ 或每个 Δ_i 为单元集. 说分划 $\Omega = \Delta_1 \cup \cdots \cup \Delta_k$ 是在群 G $(\leq S_\Omega)$ 下不变，或 G-不变的，若对每个 $g \in G$ 和每个 i, 有一个 j 使 $\Delta_i^g = \Delta_j$, 其中 $1 \leq i, j \leq k$. 明显地， Ω 上置换群 G 是非本原的当且仅当 Ω 有一个 G-不变的非平凡分划.

推论 2.5 *素数级传递群必为本原群.*

定理 2.6 *若传递群 G 具有非传递正规子群 $N \neq 1$, 则 G 非本原.*

证 设 Δ 是 N 的一个轨道. 由 N 非传递，有 $\Delta \subsetneq \Omega$. 因为 $N \lhd G$, 则对任意的 $g \in G$, Δ^g 是 $g^{-1}Ng = N$ 的轨道. 又根据 G 的传递性， $\{\Delta^g \mid g \in G\}$ 是 N 的全部轨道. 于是对任意的 $g \in G$, 或者 $\Delta = \Delta^g$, 或者 $\Delta \cap \Delta^g = \varnothing$, 这样， Δ 是 G 的块. 再由 $N \neq 1$, 有 $|\Delta| \neq 1$. 故 Δ 是 G 的非平凡块. 于是 G 非本原. □

定理 2.7 *本原群的每个非平凡正规子群必为传递群.*

这实际上是定理 2.6 的另一说法.

定理 2.8 *设 $i \in \Omega$. 则 Ω 上传递群 G 非本原 $\Longleftrightarrow$ G_i 不是 G 的极大子群.*

证 $\Longrightarrow$: 设 G 非本原， Δ 为 G 的包含 i 的一个非本原集. 令 $H = G_{\{\Delta\}}$. 由 $\{i\} \subsetneq \Delta \subsetneq \Omega$ 及 G 的传递性得 $G_i < H < G$. 于是 G_i 不是 G 的极大子群.

$\Longleftarrow$: 若有 H 满足 $G_i < H < G$, 则令 $\Delta = i^H$, 有 $\{i\} \subsetneq \Delta \subsetneq \Omega$. 只须再证明 Δ 是 G 的块: 设对某个 $g \in G$ 有 $\Delta \cap \Delta^g \neq \varnothing$, 令 $j \in \Delta \cap \Delta^g$, 可设 $j = i^{h_1} = i^{h_2 g}$, 其中 $h_1, h_2 \in H$. 于是 $i = i^{h_2 g h_1^{-1}}$, $h_2 g h_1^{-1} \in G_i < H$, 这推出 $g \in h_2^{-1} H h_1 = H$. 故 $\Delta^g = \Delta$. □

这个结果可改述为

定理 2.9 *Ω 上传递群 G 是本原的 $\Longleftrightarrow$ 对于 $i \in \Omega$, G_i 是 G 的极大子群.*

§3. 多重传递群

本节对传递性和本原性做若干重要的推广.

定义 3.1 设 $G \le S_\Omega$, 正整数 $k \le |\Omega|$. 称 G 为 k 重传递的 (或 k-传递的), 如果对 Ω 的任意两个 k 元有序子集 $(i_1, \cdots, i_k)$ 和 $(j_1, \cdots, j_k)$ 存在元素 $g \in G$ 使 $i_s^g = j_s$, $s = 1, \cdots, k$.

命题 3.2 *设 G 是 Ω 上传递群, $k > 1$, $i \in \Omega$. 则 G 在 Ω 上 k-传递 $\Longleftrightarrow$ 稳定子群 G_i 在 $\Omega - \{i\}$ 上 $(k-1)$-传递.*

证 $\Longrightarrow$: 对 $\Omega - \{i\}$ 的任意两个 $(k-1)$ 元有序子集 $(i_2, \cdots, i_k)$ 和 $(j_2, \cdots, j_k)$, 在 G 中把 $(i, i_2, \cdots, i_k)$ 变到 $(i, j_2, \cdots, j_k)$ 的元素 $g \in G_i$ 自然满足把 $(i_2, \cdots, i_k)$ 变到 $(j_2, \cdots, j_k)$.

$\Longleftarrow$: 任给 Ω 的二 k 元有序子集 $(i_1, \cdots, i_k)$ 和 $(j_1, \cdots, j_k)$. 因为 G 在 Ω 上传递, 故存在 $h \in G$ 使 $i_1^h = j_1$. 令 $i_2^h = j_2', \cdots, i_k^h = j_k'$. 由 G_{j_1} 在 $\Omega - \{j_1\}$ 上的 $(k-1)$-传递性, 存在 $l \in G_{j_1}$ 使 $(j_2')^l = j_2, \cdots, (j_k')^l = j_k$. 于是令 $g = hl$ 就有 $i_1^g = j_1$, $i_2^g = j_2, \cdots, i_k^g = j_k$. □

命题 3.3 *设 $|\Omega| = n$, G 在 Ω 上 k-传递, 则 $n(n-1)\cdots(n-k+1) \mid |G|$*

证 对 k 做归纳法. 当 $k=1$ 时, 由 $|G|=|i^G||G_i|=|\Omega||G_i|=n|G_i|$ 得 $n\mid |G|$. 对于 $k>1$, 由归纳假设及命题 3.2, 有 $(n-1)\cdots(n-k+1)\mid |G_i|$, 于是得 $n(n-1)\cdots(n-k+1)\mid |G|$. □

命题 3.4 *Ω 上的二重传递群 G 必为本原群.*

证 用反证法. 设 G 非本原且 Δ 为一非本原集, 则存在整数 i,j,k 使 $i,j\in\Delta$, $i\neq j$ 且 $k\notin\Delta$. 考虑群 G_i, 它应在 $\Omega-\{i\}$ 上传递. 但因对任意的 $g\in G_i$ 有 $\Delta\cap\Delta^g\neq\varnothing$, 故 $\Delta=\Delta^g$, 于是 $\Delta^{G_i}=\Delta$. 这说明不存在 G_i 的元素把 j 变到 k, 与 G_i 在 $\Omega-\{i\}$ 上传递相矛盾. □

定理 3.5 *设 G 在 $\Omega=\{1,2,\cdots,n\}$ 上传递, G_1 是 1 的稳定子群. 又设*

$$G=\bigcup_{i=1}^{t}G_1g_iG_1$$

是 G 关于子群 G_1,G_1 的双陪集分解, 其中 $g_1\in G_1$. 则

(1) $\Delta_i=\{1^g\mid g\in G_1g_iG_1\}$, $i=1,\cdots,t$ 是 G_1 在 Ω 上的全部轨道;

(2) G 2 重传递 $\iff$ 对任意的 $g\notin G_1$ 成立 $G_1\cup G_1gG_1=G$.

证 (1) 因为 $\Delta_i=1^{G_1g_iG_1}=(1^{g_i})^{G_1}$, 故 Δ_i 是 G_1 的轨道. 又由 G 的传递性, 有 $\bigcup_{i=1}^{t}\Delta_i=\Omega$. 最后只须证明诸 Δ_i 互不相同即可. 假定 $\Delta_i=\Delta_j$, 即 $1^{G_1g_iG_1}=1^{G_1g_jG_1}$. 于是有 $1^{g_ih}=1^{g_j}$, $h\in G_1$, 即 $g_ihg_j^{-1}\in G_1$. 这又得到 $g_i\in G_1g_jG_1$, $G_1g_iG_1=G_1g_jG_1$, 即 $i=j$.

(2) G 2 重传递 $\iff$ G_1 在 $\Omega-\{1\}$ 上传递, 即 G_1 有两个轨道 $\{1\}$ 和 $\Omega-\{1\}$. 由 (1), 这等价于 $G=G_1\cup G_1gG_1$, 对任一 $g\notin G_1$ 成立. □

下面的定理是命题 1.8 的推广.

定理 3.6 *设 G 是 Ω 上 k-传递群, $k\geq 1$, $\Delta\subseteq\Omega$, $|\Delta|=k$. 如果 $H\leq G_{(\Delta)}$, 并且满足若 $g^{-1}Hg\leq G_{(\Delta)}$, $g\in G$, 则有 $b\in G_{(\Delta)}$ 使 $g^{-1}Hg=b^{-1}Hb$, 则 $N_G(H)$ 在 $\mathrm{fix}_{\,\Omega}(H)$ 上 k-传递.*

证 令 $N=N_G(H)$, $\Gamma=\mathrm{fix}_{\Omega}(H)$. 设 $n\in N$, $\gamma\in\Gamma$, 则对任意的 $h\in H$, 有

$$(\gamma^n)^h=\gamma^{nh}=\gamma^{h'n}=\gamma^n,\ \text{对某}h'\in H.$$

于是 $\gamma^n\in\Gamma$, 即 N 可看成 Γ 上的置换群.

设 $(\gamma_1,\cdots,\gamma_k)$ 和 $(\gamma'_1,\cdots,\gamma'_k)$ 是 Γ 中的任二 k 元有序组. 由 G 的 k-传递性, 有 $x\in G$ 使 $\gamma_i^x=\gamma'_i$, $i=1,\cdots,k$. 这推出 $(\gamma'_1,\cdots,\gamma'_k)$ 被子群 H 和 H^x 所固定. 令 $\Delta=\{\delta_1,\cdots,\delta_k\}$. 又有 $y\in G$ 使 ${\gamma'}_i^y=\delta_i$, $i=1,\cdots,k$. 于是又有 $(\delta_1,\cdots,\delta_k)$ 被 H^y 和 H^{xy} 所固定. 即 $H^y\le G_{(\Delta)}$, $H^{xy}\le G_{(\Delta)}$. 由定理条件, 存在 $b\in G_{(\Delta)}$ 使 $H^{xy}=H^{yb}$, 即 $H^{xyb^{-1}y^{-1}}=H$, $xyb^{-1}y^{-1}=a\in N$. 因为

$$\begin{aligned}\gamma_i^a &= \gamma_i^{xyb^{-1}y^{-1}}={\gamma'}_i^{yb^{-1}y^{-1}}=\delta_i^{b^{-1}y^{-1}}\\ &= \delta_i^{y^{-1}}=\gamma'_i,\quad i=1,\cdots,k,\end{aligned}$$

所以 N 在 Γ 上 k-传递. □

推论 3.7 *设 G 在 Ω 上 k-传递, $k\ge 1$, $\Delta\subseteq\Omega$, $|\Delta|=k$. 则*

(1) $N_G(G_{(\Delta)})$ 在 $\mathrm{fix}_{\Omega}(G_{(\Delta)})$ 上 k-传递.

(2) 若 P 是 $G_{(\Delta)}$ 的 Sylow p-子群. 则 $N_G(P)$ 在 $\mathrm{fix}_{\Omega}(P)$ 上 k-传递.

证明留给读者.

定义 3.8 称 n 级 k-传递群 G 为 *精确 k-传递群*, 如果 $|G|=n(n-1)\cdots(n-k+1)$. 或者等价地, G 的 k 点稳定子群是单位元群.

请读者自己验证, S_n 是精确 n-传递群, 而 A_n 是精确 $(n-2)$-传递群.

定义 3.9 设 $G\le S_{\Omega}$, $|\Omega|=n$, $k\le n$. 如下递归地定义 k 重本原性: 称 G 是 1-本原的, 如果 G 是本原群; 称 G 是 k-本原的, $k>1$, 如果 G 传递, 并且点稳定子群 G_i 在 $\Omega-\{i\}$ 上是 $(k-1)$-本原的.

事实上， S_n 和 A_n 也分别为 n-本原群和 $(n-2)$-本原群.

定义 3.10 设 $G \leq S_\Omega$, $|\Omega| > 1$. 称 G 为 $\frac{1}{2}$-传递群, 如果 $G \neq 1$, 且 G 在 Ω 上的所有轨道等长. 如果 $|\Omega| = 1$, 我们也称 G 为 $\frac{1}{2}$-传递群.

还可递归地定义 $(k+\frac{1}{2})$-传递性, 请读者自己给出它的定义.

下面我们给出几个多重传递群的例子. 它们是从有限域上的向量空间的线性变换群中得到的. 为叙述它们, 我们先把有限域及线性代数的若干概念复习一下. 这些知识在以后还要用到.

关于有限域的基本知识, 主要有下面的

定理 3.11 (1) 设 $\mathbf{F}$ 是 q 个元素的域, 则 $q = p^r$, p 是素数. 并且在同构的意义下只存在一个 q 个元素的域, 把它记作 $\mathbf{F} = GF(q)$ 或 $GF(p^r)$, 且有 $\operatorname{char} \mathbf{F} = p$.

(2) $GF(q)$ 的乘法群是 $q-1$ 阶循环群, 其生成元叫域 $GF(q)$ 的本原元素.

(3) $GF(p^r)$ 的自同构群是 r 阶循环群, 由自同构 $x \mapsto x^p$, $x \in GF(p^r)$, 生成.

(4) 对每个 $s|r$, $GF(p^r)$ 存在唯一的子域 $GF(p^s)$, 并且它只有这些子域.

(证明从略.)

设 $V = V(n, \mathbf{F})$ 是域 $\mathbf{F}$ 上 n 维向量空间, $0 \neq v \in V$, 我们以 $\langle v \rangle$ 表示由 v 生成的一维子空间.

定义 3.12 设 $\mathbf{F}$ 是域, $V = V(n, \mathbf{F})$ 是 $\mathbf{F}$ 上 n 维向量空间. 称 V 的所有一维子空间的集合 $P = PG(n-1, \mathbf{F})$ 为 $\mathbf{F}$ 上 $n-1$ 维射影空间. P 中的元素叫做点. 特别地, 若 $n = 2$, $P = PG(1, \mathbf{F})$ 叫 $\mathbf{F}$ 上的射影直线. 它里面的元素 $\langle (x, 1) \rangle$, $x \in \mathbf{F}$, 简记作 x, 而 $\langle (1, 0) \rangle$ 简记作 ∞, 于是可认为 $P = \mathbf{F} \cup \{\infty\}$.

明显地，V 的满秩线性变换 $\alpha \in GL(n,\mathbf{F})$ 可以看作 $P = PG(n-1,\mathbf{F})$ 的一个一一变换. 并且 α 保持 P 中每点不变 $\Longleftrightarrow$ α 是数乘变换，即 $\alpha \in Z = Z(GL(n,\mathbf{F}))$. 因此 $PGL(n,\mathbf{F}) = GL(n,\mathbf{F})/Z$ 和 $PSL(n,\mathbf{F}) = SL(n,\mathbf{F})/Z \cap SL(n,\mathbf{F})$ 都可看作 P 的变换群.

命题 3.13 $PSL(n,\mathbf{F})$, $n \geq 2$, 作为 $PG(n-1,\mathbf{F})$ 上的置换群是 2 重传递的.

证 任取 $PG(n-1,\mathbf{F})$ 中两对不同的点 $\langle v_1\rangle, \langle v_2\rangle$ 和 $\langle v_1'\rangle, \langle v_2'\rangle$, 其中 $v_i, v_i' \in V = V(n,\mathbf{F})$. 于是有 v_1 和 v_2 (以及 v_1' 和 v_2') 线性无关，这时自然可取 $\alpha \in SL(n,\mathbf{F})$ 使

$$v_1^\alpha = v_1',\ v_2^\alpha = \lambda v_2',\ \lambda \in \mathbf{F}^\#.$$

(对于 $n \geq 3$, 还可取到 α 使 $\lambda = 1$.) 则 α 作为 $PG(n-1,\mathbf{F})$ 的变换即把 $\langle v_1\rangle, \langle v_2\rangle$ 变到 $\langle v_1'\rangle, \langle v_2'\rangle$. □

由此命题，自然 $PGL(n,\mathbf{F})$ 在 P 上也是 2 重传递的. 当 $n \geq 3$, 我们有 $PGL(n,\mathbf{F})$ 在 P 上不是 3-传递的. (证之 !) 但对 $n = 2$, 我们有

例 3.14 $PGL(2,p^r)$ 在 $P = PG(1,p^r)$ 上是精确 3-传递的. 于是 $|PGL(2,p^r)| = (p^r+1)p^r(p^r-1)$.

证明留给读者

定义 3.15 设 $V = V(n,\mathbf{F})$ 是域 $\mathbf{F}$ 上 n 维向量空间. 设 $\alpha \in GL(n,\mathbf{F})$, $a \in V$. 则变换 $x \mapsto x^\alpha + a$, $\forall x \in V$, 叫做 V 的仿射变换. V 的全体仿射变换的集合记作 $AGL(n,\mathbf{F})$. 明显地，$AGL(n,\mathbf{F})$ 在变换乘法之下作成一群，它包含 $GL(n,\mathbf{F})$ 为其子群.

请读者自己研究下面两个例子.

例 3.16 (1) 设 $\mathbf{F}=GF(p^r), V=V(n,p^r)$ 是 $\mathbf{F}$ 上 n 维向量空间, $n>1$. 则 $AGL(n,p^r)=AGL(n,\mathbf{F})$ 作为 V 上的置换群是 2 重传递的, 并且包含正则交换正规子群

$$T=\{\tau\in AGL(n,p^r)\mid x^\tau=x+b,\ b\in V\}.$$

若 $AGL(n,p^r)$ 是双本原的, 则有 $p^r=2$, 且这时, $AGL(n,p^r)$ 是 3-传递的. 又, $AGL(n,p^r)$ 是 $\frac{5}{2}$-传递的 $\Longleftrightarrow$ $p^r=2$.

(2) 设 $\mathbf{F}=GF(p^r)$. 以 $A\Gamma L(1,p^r)$ 表 $\mathbf{F}$ 的下列形状的变换的全体: $x\mapsto ax^\tau+b$, $\forall x\in\mathbf{F}$, 其中 $a,b\in\mathbf{F}$, $a\neq 0$, τ 是 $\mathbf{F}$ 的任一自同构. 则 $A\Gamma L(1,p^r)$ 作为 $\mathbf{F}$ 上置换群是可解 2 重传递群, $|A\Gamma L(1,p^r)|=p^r(p^r-1)r$. 并有

$$\begin{aligned}
&A\Gamma L(1,p^r)\ 3\text{-传递} &&\Longleftrightarrow && p^r=3 \text{ 或 } 4;\\
&A\Gamma L(1,p^r)\text{双本原} &&\Longleftrightarrow && p^r=2 \text{ 或 } p^r-1 \text{ 是素数};\\
&A\Gamma L(1,p^r)\ \frac{5}{2}\text{-传递} &&\Longleftrightarrow && p^r=3 \text{ 或 } p=2, r \text{ 是素数}.
\end{aligned}$$

从以上的例子我们已经看出, 存在无穷多个不是对称群和交错群的 2-传递和 3-传递群. 但若传递重数高于 3, 则只发现了四个多重传递群 ($\neq S_n, A_n$). 它们是上世纪六十年代发现的 Mathieu 群, 将在 §7 中讲述.

§4. 轨道图

本节考虑 Ω 上的本原群, 重点是讨论 G_α 在 Ω 上的各轨道长度以及 G_α 在各轨道上的传递成分.

先设 G 为 Ω 上的传递群. 令 $\Omega^2=\Omega\times\Omega=\{(\alpha,\beta)\mid\alpha,\beta\in\Omega\}$. G 自然地作用于 Ω^2 上: 若 $(\alpha,\beta)\in\Omega^2, g\in G$, 则 $(\alpha,\beta)^g=(\alpha^g,\beta^g)$. G 在 Ω^2 上的轨道个数 r 称为 G 的秩. $\Delta_0=\{(\alpha,\alpha)\mid\alpha\in\Omega\}$ 显然是一个轨道. 设 $\Delta_0, \Delta_1, \cdots, \Delta_{r-1}$ 是 G 在 Ω^2 上的全部轨道.

取定 $\alpha\in\Omega$, 定义集合

$$\Delta_i(\alpha)=\{\beta\mid(\alpha,\beta)\in\Delta_i\},\quad i=0,1,2,\cdots,r-1.$$

因 G 传递，所以每个 $\Delta_i(\alpha)$ 都不空. 又若 $\beta \in \Omega$, (α,β) 属于且只属于一个轨道 Δ_i. 所以 $\Delta_0(\alpha)$, $\Delta_1(\alpha)$, $\cdots$, $\Delta_{r-1}(\alpha)$ 是两两不相交的集合，而它们的并为 Ω. 显然 $\Delta_0(\alpha)=\{\alpha\}$. 于是我们有

命题 4.1 *$\Delta_0(\alpha), \Delta_1(\alpha), \cdots, \Delta_{r-1}(\alpha)$ 是 G_α 在 Ω 上的全部轨道. 并且若 $g \in G$. 那么 $\Delta_i(\alpha^g)=\Delta_i(\alpha)^g$, $i=0,1,\cdots,r-1$.*

$\Delta_0(\alpha)$, $\Delta_1(\alpha)$, $\cdots$, $\Delta_{r-1}(\alpha)$ 称为 G 的 次轨道. 其长度 $n_i=|\Delta_i(\alpha)|$ 称为 G 的次级数. 显然 $n_0=1$. 今后我们这样排列 $\Delta_i(\alpha)$ 的次序，使 $n_0=1 \le n_1 \le n_2 \le \cdots \le n_{r-1}$. 易知 G 的秩为 2 当且仅当 G 为 2-传递的. 在本节以后的讨论中，总假定 G 的秩大于 2.

对 G 在 Ω^2 上的轨道 Δ_i, $i>0$, 显然 $\Delta_i^*=\{(\alpha,\beta) \mid (\beta,\alpha) \in \Delta_i\}$ 也是一个轨道. 于是有 j 使 $\Delta_i^*=\Delta_j$. 此时称 $\Delta_i^*=\Delta_j$ 为与 Δ_i配对的轨道. 显然 $(\Delta_i^*)^*=\Delta_i$. 如果 $\Delta_i^*=\Delta_i$, 则称 Δ_i 为自配对的. 相应地， $\Delta_i^*(\alpha)$ 称为 与 $\Delta_i(\alpha)$ 配对的轨道. 而若 Δ_i 为自配对的，也称 $\Delta_i(\alpha)=\Delta_i^*(\alpha)$ 为自配对的. 下面的引理是明显的.

引理 4.2 *若 $\Delta_i(\alpha), i>0,$ 是自配对的, 则对任意的 $\beta \in \Delta_i(\alpha)$, 存在一个元素 $g \in G$, 使 g 的轮换分解式中含有一个对换 $(\alpha\ \beta)$, 即 $g=(\alpha\ \beta)\cdots$. 反之亦然. 因此 G 有自配对的次轨道当且仅当 G 为偶阶群.*

为定义轨道图，我们回忆一下图论的某些概念 (可参见 XIV, §1). (V,E) 称为 有向图, 如果 V 为有限集合，而 E 为 $\Omega\times\Omega$ 的一个子集合. V 中元素叫做 顶点, E 中元素称为 有向边或弧. 若 (α,β) 为弧，则 α,β 分别称为 (α,β) 的起点和终点. 注意有可能 $(\alpha,\beta)\in E$ 而 $(\beta,\alpha)\notin E$. $|V|$ 称为 图 (V,E) 的阶. 我们还常用 V 来称图 (V,E), 这当然是在 E 已明确的情况下. 若 $\alpha\in V$, 以 α 为起点的弧的个数称为 α 的出度, 同样可以定义 α 的 入度. 一个图称为正则图, 如果图的各顶点的入度，出度都等于一个共同的数 d. 此时 d 称为 正则图的度. 设图 (V,E) 已给定, 所谓 长为 l 的路 是指一个顶点组成的序列 $\alpha=\alpha_0,\alpha_1,\cdots,\alpha_l=\beta$, 其中对每个 i, $1\le i\le l$, $(\alpha_{i-1},\alpha_i)\in E$ 或 $(\alpha_i,\alpha_{i-1})\in E$. 若 $\alpha_0=\alpha_l$, 这条路叫做 圈. 如果

在路中所有的 (α_{i-1},α_i) 都属于 E, 则称 $\alpha=\alpha_0,\alpha_1,\cdots,\alpha_l=\beta$ 为有向路. 相应地有有向圈的概念. 在图的顶点集合 V 上定义关系"$\sim$": $\alpha\sim\beta$ 当且仅当从 α 到 β 有一条路. 此时"$\sim$"是等价关系. 关系 $\sim$ 的等价类 C 以及 $E\cap(C\times C)$ 决定一个图, 称为 V 的连通分支. 如果这个连通分支就是 (V,E), 则 (V,E) 称为 *连通的*. 一个连通图称为 *强连通的*, 如果对一切 $\alpha,\beta\in V$, 总有一条自 α 到 β 的有向路.

设 (V,E) 为一个图. V 的置换 g 叫做 *图 (V,E) 的自同构*, 如果当 (α,β) 为弧时, (α^g,β^g) 也为弧. (V,E) 的全部自同构组成一个群, 叫做 *该图的自同构群*. 设 G 为 (V,E) 的自同构群的一个子群, 若 G 为 V 上传递群, 则称 G *是点传递的*. 下面的引理在以下的讨论中要用到.

引理 4.3 *若连通图 (V,E) 的自同构群 G 是点传递的, 则 (V,E) 为强连通的.*

证 只需证对任意的 $\alpha,\beta\in V$, $(\alpha,\beta)\in E$, 则由 β 到 α 有一条有向路. 对每个 $\gamma\in V$, 定义集合

$$V_\gamma=\{\delta \mid \text{由 } \gamma \text{ 到 } \delta \text{ 有一条有向路}\}.$$

由于 G 是点传递的, 所以有 $g\in G$ 使 $\alpha^g=\beta$. 此时 $V_\alpha^g=V_\beta$, 于是知 $|V_\alpha|=|V_\beta|$. 如果由 α 到 β 有有向路, 我们有 $V_\beta\subseteq V_\alpha$. 这样一来得 $V_\alpha=V_\beta$. 但显然 $\alpha\in V_\alpha$, 从而 $\alpha\in V_\beta$. 引理成立. □

今设 G 为 Ω 上的传递群. $\Delta_0,\Delta_1,\cdots,\Delta_{r-1}$ 为 G 在 Ω^2 上的轨道. 对每个 $i>0$, (Ω,Δ_i) 为一个图. 它称为 G *的轨道图*. G 的每个元素都是 (Ω,Δ_i) 的自同构. 这说明 G 是 $r-1$ 个图 (Ω,Δ_i), $i>0$, 的自同构群的共同的子群. 在图论中把任意两个顶点 α,β 之间都有有向弧 (α,β) 的图叫做 *完全有向图*. 在我们的情形, 把所有的轨道图拼起来就得到完全有向图. 为区分这些子图 (Ω,Δ_i), 我们准备 $r-1$ 种颜色. 如果 (α,β) 是 (Ω,Δ_i) 的弧, 则说 (α,β) *是带第 i 种颜色的*. 这样得到的完全图称为 *着色的完全图*. G 是这个着色完全图的自同构组成的群.

定理 4.4 设 G 为 Ω 上的传递群. G 在 Ω 上本原当且仅当 G 的每个轨道图都是连通图. 此时各轨道图都是强连通图.

证 若 $\Gamma \subset \Omega$ 为轨道图 (Ω, Δ_i) 的一个连通分支. 易知 Γ^g 也是一个连通分支, 因为 g 把 Γ 中每条路变成 Γ^g 中的一条路. 这样一来, 若 $\Gamma \cap \Gamma^g \neq \varnothing$, 则 $\Gamma = \Gamma^g$. 也即 Γ 为一个块. 如果 G 为本原群, 注意到连通分支 Γ 中至少有两个顶点, $\Gamma = \Omega$. 这证明了本原群的每个轨道图都是连通图.

如果 G 为非本原群, 而 Σ 为 G 的非本原集. 取 $\alpha, \beta \in \Sigma$, 并设 $(\alpha, \beta) \in \Delta_i$. 我们证明由 α 出发的 (Ω, Δ_i) 中的任一条路 $\alpha = \alpha_0, \alpha_1, \cdots, \alpha_u$ 的顶点都属于 Σ. 这一点对 α_0 是正确的. 若已知 $\alpha_j \in \Sigma$, 由于 $(\alpha_j, \alpha_{j+1}) \in \Delta_i$ 或 $(\alpha_{j+1}, \alpha_j) \in \Delta_i$, 所以有 $g \in G$, 使 $\alpha^g = \alpha_j$ 且 $\beta^g = \alpha_{j+1}$ 或者 $\alpha^g = \alpha_{j+1}$, $\beta^g = \alpha_j$. 这说明 $\alpha_j \in \Sigma^g$. 因此 $\Sigma = \Sigma^g$, 故 $\alpha_{j+1} \in \Sigma$. 于是 (Ω, Δ_i) 的包含 α 的连通分支在 Σ 中. 故 (Ω, Δ_i) 是不连通的. □

注: 上边定理实际上证明了传递群 G 的每个轨道图的连通分支 Σ 都是 G 的块.

这个定理有以下有用的推论.

推论 4.5 设 G 为 Ω 上本原群, $\alpha \neq \beta \in \Omega$. Γ 为 Ω 的一子集且 $\varnothing \subsetneqq \Gamma \subsetneqq \Omega$. 则 G 中有元素 g, 使 $\alpha^g \in \Gamma$, 而 $\beta^g \notin \Gamma$.

证 设 $(\alpha, \beta) \in \Delta_i$, G 的本原性推出图 (Ω, Δ_i) 是强连通的. 所以若 $\gamma \in \Gamma$ 而 $\delta \notin \Gamma$, 由 γ 到 δ 有一条路 $\gamma = \gamma_0, \gamma_1, \cdots, \gamma_s = \delta$, 其中 $(\gamma_j, \gamma_{j+1}) \in \Delta_i$ 对 $j = 0, 1, \cdots, s-1$ 成立. 于是有一点 $\gamma_k \in \Gamma$, 而 $\gamma_{k+1} \notin \Gamma$. 因为 $(\gamma_k, \gamma_{k+1}) \in \Delta_i$, 所以有 $g \in G$, 使 $\alpha^g = \gamma_k \in \Gamma$ 而 $\beta^g = \gamma_{k+1} \notin \Gamma$. □

推论 4.6 设 G 为 Ω 上的传递群, U 为 G 的子群. 若 U 在 Ω 上有一个轨道 Γ 满足: $|\Gamma| > \frac{1}{2}|\Omega|$ 且 U^Γ 为本原的, 则 G 在 Ω 上是本原群.

证 任取 G 的轨道图 (Ω, Δ_i) 的一个连通分支 Σ. 也用 Σ 表示其顶点集合. 如果 $|\Gamma \cap \Sigma| \geq 2$, 则有 $\alpha, \beta \in \Sigma \cap \Gamma$. (α, β) 属于 U

在 Γ^2 上的某轨道. 由于 U 在 Γ 上为本原群, 所以相应的 U 的轨道图是连通的. 这说明 Γ 整个地包含在 Σ 内. 这时由于 $|\Gamma| > \frac{1}{2}|\Omega|$, 同时 Σ 作为 G 的块, $|\Sigma| \mid |\Omega|$, 故 $\Sigma = \Omega$. 如果 (Ω, Δ_i) 的每个连通分支与 Γ 的交不超过一点, 那么 (Ω, Δ_i) 的连通分支个数应不小于 $|\Gamma| > \frac{1}{2}|\Omega|$. 这使得每个连通分支只有一点, 而这是不可能的. □

用轨道图的方法可得到下列几个关于本原群的重要定理.

定理 4.7 *设 G 为 Ω 上本原群但非正则群. $\alpha \in \Omega$, 设 G_α 的轨道长度为 $1 = n_0 \leq n_1 \leq n_2 \leq \cdots \leq n_{r-1}$. 则 $n_1 > 1$, 且对一切 $j, 1 \leq j \leq r-2, n_{j+1} \leq (n_1 - 1)n_j$.*

证 先证 $n_1 > 1$. $n_1 = 1$ 意味着轨道图 (Ω, Δ_1) 是一些有向圈之并. 在 G 是本原群时 (Ω, Δ_1) 还是包含 Ω 中全部点的有向图. 此时若 $\alpha \in \Omega$, 则 G_α 把 Ω 中每个点都不变, 因而 $G_\alpha = 1$, 这与 G 不是正则群的假设矛盾. 从而 $n_1 > 1$.

用反证法证明第二个结论. 设有 j 使 $n_{j+1} > (n_1 - 1)n_j$. 令 $\Gamma = \Delta_0(\alpha) \cup \Delta_1(\alpha) \cup \cdots \cup \Delta_j(\alpha)$. 则 $\Gamma \subsetneqq \Omega$.

Ω 上的顶点序列 $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_m$ 称为一条交错路, 如果当 u 为偶数时 $(\alpha_u, \alpha_{u+1}) \in \Delta_1$, 而当 u 为奇数时 $(\alpha_u, \alpha_{u+1}) \in \Delta_1^*$. 我们证明对任何 $\beta \in \Omega$, 都有一条从 α 到 β 的交错路. 取 $\gamma \in \Delta_1(\alpha)$, 由于 $|\Delta_1^*(\gamma)| = n_1$, 故有一点 $\delta \in \Delta_1^*(\gamma)$ 且 $\delta \neq \alpha$. 此时 α, γ, δ 为一条交错路. 设 $(\alpha, \delta) \in \Delta_k$, 由于 (Ω, Δ_k) 是强连通的, 所以有一条路 $\beta_0 = \alpha, \beta_1, \cdots, \beta_m = \beta$, 其中对每个 i, $(\beta_i, \beta_{i+1}) \in \Delta_k$. 于是有 γ_i 使 $(\beta_i, \gamma_i) \in \Delta_1$, 而 $(\gamma_i, \beta_{i+1}) \in \Delta_1^*$. 把每个 γ_i 置于 β_i 和 β_{i+1} 之间就得到 α 到 β 的交错路.

今取 $\beta \notin \Gamma$, 并设 $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_m = \beta$ 为从 α 到 β 的最短的一条交错路. 此时 $\alpha \in \Gamma$ 而 $\beta \notin \Gamma$, 因而总有一个 $l, 1 \leq l \leq m-1$, 使 $\alpha_l \in \Gamma$, 而 $\alpha_{l+1} \notin \Gamma$. 设 $\alpha_{l-1} \in \Delta_u(\alpha)$, $\alpha_l \in \Delta_s(\alpha)$, $\alpha_{l+1} \in \Delta_t(\alpha)$. 由于 $\alpha_l \in \Gamma$ 而 $\alpha_{l+1} \notin \Gamma$, 所以 $s \leq j$, $j+1 \leq t$, 从而 $s \neq t$. 同时 $u \neq t$, 否则 $\Delta_u(\alpha) = \Delta_t(\alpha)$, 从 α 到 α_{l+1} 将有一条长为 $l-1$ 的交错路, 因而从 α 到 β 有一条更短的交错路. 这与我们的假设

矛盾. 今设 l 为偶数. 对 $\delta \in \Delta_t(\alpha)$, 有 $\gamma \in \Delta_s(\alpha)$, 使 $(\gamma,\delta) \in \Delta_1$ 即 $\delta \in \Delta_1(\gamma)$. 这说明 $\Delta_t(\alpha)$ 包含在 $\bigcup_{\gamma\in\Delta_s(\alpha)} (\Delta_1(\gamma) \cap \Delta_t(\alpha))$ 内. 但因 $(\alpha_l, \alpha_{l-1}) \in \Delta_1$, 所以 $|\Delta_1(\alpha_l) \cap \Delta_t(\alpha)| \leq n_1 - 1$, 从而对一切 $\gamma \in \Delta_s(\alpha)$, $|\Delta_1(\gamma) \cap \Delta_t(\alpha)| \leq n_1 - 1$. 于是 $n_t = |\Delta_t(\alpha)| \leq (n_1-1)n_s$. 但 $s \leq j < j+1 \leq t$, 故 $n_{j+1} \leq n_t \leq (n_1-1)n_s \leq (n_1-1)n_j$. 这推出了矛盾. □

定理 4.8 设 G 为 Ω 上非正则本原群, 其次级数 n_i, n_j 互素, $1 \leq i,j \leq r-1$. 则 G_α 有一个长为 n_k 的轨道, 使 $n_k \mid n_i n_j$, 而且 $n_k > n_i$, $n_k > n_j$.

证 设 $|\Delta_i(\alpha)| = n_i$, $|\Delta_j(\alpha)| = n_j$ 且 $n_i < n_j$. 仍用 Δ_i, Δ_j 表示 G 在 Ω^2 上的相应轨道. 考虑三点集 $(\alpha', \beta', \gamma')$, 其中 $\alpha', \beta', \gamma' \in \Omega$ 而 $(\alpha', \beta') \in \Delta_i$, $(\beta', \gamma') \in \Delta_j$. 把这些三点集所成的集合记作 Θ, 其中的三点集叫做 Θ-路. 由于 β' 有 $n = |\Omega|$ 种取法, 而当 β' 取定后 α', γ' 各有 n_i, n_j 个取法. 所以 $|\Theta| = nn_in_j$. 此时有

1) G 在 Θ 上传递.

取定一个 Θ-路 $(\alpha', \beta', \gamma')$. 它的稳定子群为 $G_{\alpha'\beta'\gamma'}$, 显然 $G > G_{\alpha'} > G_{\alpha'\beta'} > G_{\alpha'\beta'\gamma'}$. $|G : G_{\alpha'}| = |G : G_{\beta'}| = n$. 又 $\beta' \in \Delta_i(\alpha')$, 所以 $|G_{\alpha'} : G_{\alpha'\beta'}| = n_i$, 因而 $|G_{\beta'} : G_{\alpha'\beta'}| = n_i$. 同理 $|G_{\beta'} : G_{\beta'\gamma'}| = n_j$ 而 $G_{\beta'\gamma'} \cap G_{\alpha'\beta'} = G_{\alpha'\beta'\gamma'}$. 故 n_i, n_j 都是 $|G_{\beta'} : G_{\alpha'\beta'\gamma'}|$ 的因子. 而 $(n_i, n_j) = 1$, 所以 $n_in_j \mid |G_{\beta'} : G_{\alpha'\beta'\gamma'}|$. 这推出 $|G : G_{\alpha'\beta'\gamma'}|$ 为 nn_in_j 的倍数. 但 $|G : G_{\alpha'\beta'\gamma'}| \leq |\Theta|$, 所以 G 在 Θ 上传递.

2) 取定 α, 则 $\Delta(\alpha) = \{\gamma \mid \exists \beta \in \Omega, \text{使 } (\alpha,\beta,\gamma) \in \Theta\}$ 为次轨道.

这由 G 在 Θ 上传递立即推出.

记 $\Delta(\alpha) = \Delta_k(\alpha)$ 且 $n_k = |\Delta_k(\alpha)|$.

3) $n_k \mid n_in_j$.

若 $\gamma, \gamma' \in \Delta_k(\alpha)$, 则有 $g \in G_\alpha$ 使 $\gamma^g = \gamma'$. g 把以 α 为起点 γ 为终点的每条 Θ-路变成以 α 为起点 γ' 为终点的一条 Θ-路. 所以

有一个正数 x, 对一切 $\gamma\in\Delta_k(\alpha)$, 从 α 到 γ 的 Θ-路恰好有 x 条. 于是我们得到 $n_in_j=xn_k$. 即 $n_k \mid n_in_j$.

4) $n_k>n_j$.

取定 α 后, 只要 $\beta\in\Delta_i(\alpha)$, $\gamma\in\Delta_j(\beta)$, (α,β,γ) 就在 Θ 内, 这说明只要 $\beta\in\Delta_i(\alpha)$, 就有 $\Delta_j(\beta)\subseteq\Delta_k(\alpha)$. 因而 $n_j\le n_k$. 而等号成立意味着对 $\beta\in\Delta_i(\alpha)$, $\Delta_j(\beta)=\Delta_k(\alpha)$. 此时 $\Delta_j(\beta)$ 同时在 G_α 下和 G_β 下不变, 因而在 $G=\langle G_\alpha,G_\beta\rangle$ 下不变. 这只能 $\Delta_j(\beta)=\Omega$, 而这是不可能的. □

推论 4.9 非正则本原群的次级数 $n_0=1<n_1\le\cdots\le n_{r-1}$ 中任一个 $n_j, j\ge1$, 和最大次级数 n_{r-1} 不能互素.

按定理 4.8 的同样的想法可以证明下面的定理 4.10.

定理 4.10 设 G 为 Ω 上本原但非 2 重传递群, $\alpha\in\Omega$. $\Sigma\ne\{\alpha\}$ 为 G_α 的一个轨道. 若 G_α^Σ 在 Σ 上 2 重传递, 则 G_α 有一个轨道长为 l, 其中 $l \mid k(k-1)$ 且 $l\ge 2(k-1)$, 其中 $k=|\Sigma|$.

证明留作习题.

设 G 为 Ω 上的本原群, $\Gamma\ne\{\alpha\}$ 为 G_α 的一个轨道. 我们考察传递成分 G_α^Γ.

引理 4.11 设 G 的子群 $Y\ne1$ 有至少一个不动点, 那么 G 中有元素 g, 使 $X=Y^g\le G_\alpha$ 且 $X^\Gamma\ne1$.

证 用 Φ 表示 Y 的不动点集. 由于 $Y\ne1$, Φ 为 Ω 的非空真子集. 取 $\gamma\in\Gamma$. 由于 G 是本原群, 由推论 4.5 知有 $g\in G$, 使 $\alpha\in\Phi^g$, 而 $\gamma\notin\Phi^g$. 令 $X=Y^g$. 则 $X\le G_\alpha$, 而 γ 不是 X 的不动点, 即 $X^\Gamma\ne1$. □

定理 4.12 若 G 为 Ω 上本原群, $\Gamma\ne\{\alpha\}$ 为 G_α 的一个轨道, 则 G_α 的每个合成因子都是 G_α^Γ 的某子群的合成因子.

证 设 K 为 G_α 的合成因子. 在 G_α 中选取一子群 Y, 使 K 为 Y 的合成因子但不是 Y 的任何真子群的合成因子. 根据 4.11,

我们有 $g\in G$, 使 $1\neq X=Y^g\leq G_\alpha$, $X^\Gamma\neq 1$. X 在 Γ 上作用的核 $X_{(\Gamma)}$ 是 X 的真子群, 所以 K 不是 $X_{(\Gamma)}$ 的合成因子. 于是 K 是 X^Γ 的合成因子. □

这个定理可以提出许多事实.

推论 4.13 (1) *设 G 为 Ω 上本原群, $\alpha\in\Omega$, $\Delta_i(\alpha)$, $i>0$, 为 G_α 的一个轨道. 若 $G_\alpha^{\Delta_i(\alpha)}$ 可解, 则 G_α 可解.*

(2) *在 (1) 的假设下, 若 $G_\alpha^{\Delta_i(\alpha)}$ 为 p-群, 其中 p 为素数, 则 G_α 为 p-群.*

(3) *若 G_α 有一个长度为素数 p 的轨道, 那么它是 G_α 的异于 $\{\alpha\}$ 的最短的轨道.*

在本节最后我们看一些例子.

例 4.14 本原群 G 有一个次轨道长度为 2, 则 G 同构于 $2p$ 阶二面体群, 其中 p 为奇素数.

证 由定理 4.7 知 $n_1=2$, 且一切 $n_{j+1}\leq(2-1)n_j$. 所以 G_α 的轨道除去 $\{\alpha\}$ 外都有长度 2. 此时由推论 4.13, G_α 为 2-群. 我们断言, 对 $\alpha\neq\beta\in\Omega$, $G_{\alpha\beta}=1$. 否则设 $1\neq x\in G_{\alpha\beta}$ 为 2 阶元, $x=(\alpha)(\beta)(\gamma,\delta)\cdots$, 此时 $\{\gamma,\delta\}$ 为 G_α 的也为 G_β 的轨道. 这样一来 $\{\gamma,\delta\}$ 是 G_α-不变的, 也是 G_β-不变的, 因而是 $\langle G_\alpha,G_\beta\rangle$-不变的. 但 G 非正则, 所以 $G=\langle G_\alpha,G_\beta\rangle$. 这是不可能的. 所以 $|G_\alpha|=2$, 此时 $G=\langle G_\alpha,G_\beta\rangle$ 为两个 2 阶元素生成的群, 故为二面体群, 其阶为 $2n$, 且有一个 n 阶子群 N, N 中任意子群都是 G_α-不变的. 因 G 本原, 所以 $n=|N|$ 为素数 p. 因 $G_{\alpha\beta}=1$, 每个 2 阶元仅有一个不动点, 所以 p 为奇素数. □

例 4.15 设 $n=|\Sigma|\geq 5$, G 为 Σ 上交错群, 考察 G 在 Σ 中的无序二元子集上的作用.

解 设 $\Sigma=\{1,2,\cdots,n\}$. 以 Ω 表 Σ 中无序二元子集所成的集合, 则 $|\Omega|=\frac{n(n-1)}{2}$. 给定 $\alpha=\{1,2\}$, 则 $G_\alpha\cong(Z_2\times S_{n-2})\cap A_n$.

取集合

$$\Gamma_1 = \{\{i,j\} \mid |\{i,j\} \cap \{1,2\}| = 1\},$$

$$\Gamma_2 = \{\{i,j\} \mid \{i,j\} \cap \{1,2\} = \varnothing\}.$$

容易看出，Γ_1, Γ_2 为 G_α 的轨道. 其长度分别为 $|\Gamma_1| = 2(n-2)$ 和 $|\Gamma_2| = \frac{(n-2)(n-3)}{2}$. 显然 $\{\alpha\}, \Gamma_1, \Gamma_2$ 是 G_α 的全部轨道. 因而 G 在 Ω 上的秩为 3.

当 $n = 5$ 时, 知 A_5 可表示成 10 阶本原群, 其次级数为 $1, 3, 6$.
□

例 4.16 若 $n = 6, 8$ 或 12, 则 n 级本原群一定是二重传递群.

证 由例 4.14. 知这样的群 G 的非平凡次轨道长度大于 2. 又在我们的情况下 $p = n - 1$ 为素数. 这说明 G 不能是秩 3 的, 否则 $n_1 + n_2 = p$, $(n_1, n_2) = 1$. 这与推论 4.9 矛盾. 这样一来若 G 非 2-传递的, 则 G 的秩 $r \geq 4$, $n_1 \geq 3$, 故 $n \geq 1 + 3(r-1) \geq 10$. 这说明当 $n = 6$ 或 8 时 n 阶本原群为 2-传递群. 今设 $n = 12$, G 非 2-传递. 由于 $r \geq 4$, 故 $n_1 \leq \frac{11}{3}$ 从而 $n_1 = 3$. 而其它次轨道的长度不能全部是 3 的倍数, 这推出最大次轨道长度 $n_{r-1} \geq 6$. 这样一来剩下的次级数之和为 2, 这是不可能的. □

例 4.17 决定 10 级的非 2-传递的本原群.

解 设 $|\Omega| = 10$, G 为 Ω 上非 2-传递的本原群. 取 $\alpha \in \Omega$. 考虑 G_α 的次轨道长度 $n_1, n_2, \cdots$. 除去 $\{\alpha\}$ 外, 其余次轨道长度之和为 9. 所以有一个奇数 l 长的次轨道. 若 $l = 5$ 或 7, 由推论 4.13.3) 知 $n_1 = 5$ 或 7. 而这是不可能的. 故此时 $l = 3$ 而且 $n_1 = 3$. 若 $G_\alpha^{\Delta_1(\alpha)} \cong Z_3$, 则 G_α 为 3-群, G 的阶是一个奇数的两倍. 此时 G 中有一个奇数阶的正规子群 N. 因 G 本原, 故 N 传递. 但 $|N| \not\equiv 0 (\mathrm{mod}\ 10)$, 矛盾. 故 $G_\alpha^{\Delta_1(\alpha)}$ 在 $\Delta_1(\alpha)$ 上 2-传递. 由定理 4.10 知 G_α 中有一个轨道长度为 l, 且 $l \mid 6$ 和 $l \geq 4$. 因此 $l = 6$. 所以 G 的秩为 3, 次级数为 $1, 3, 6$.

设 $|\Delta_1(\alpha)| = 3$, $|\Delta_2(\alpha)| = 6$. 由于 $G_\alpha^{\Delta_1(\alpha)} \cong S_3$. 故对 $\beta \in \Delta_1(\alpha)$. $G_{\alpha\beta}$ 在 $\Delta_1(\alpha) - \{\beta\}$ 上传递. 所以要么 $\Delta_1(\alpha) - \{\beta\} \subseteq \Delta_1(\beta)$,

要么 $\Delta_1(\beta)-\{\alpha\}\subseteq\Delta_2(\alpha)$. 前者与轨道图 (Ω,Δ_1) 的连通性相抵触，而后者说明 $\Delta_2(\alpha)=\bigcup\limits_{\beta\in\Delta_1(\alpha)}(\Delta_1(\beta)-\{\alpha\})$. 由于 $|\Delta_(\alpha)|=6$, 这还是一个无交并. 记 $K=(G_\alpha)_{(\Delta_1(\alpha))}$ 为 G_α 在 $\Delta_1(\alpha)$ 上的核. 若 $1\neq k\in K$, 则 k 应保持每个二元子集 $\Delta_1(\beta)-\{\alpha\}$ $(\beta\in\Delta_1(\alpha))$ 不动. 所以 k 为 2 阶元. 于是由定理 4.11, k 有一个共轭元 $k^x=(\beta_1,\beta_2)\cdots\in G_\alpha$, 其中 $\beta_1,\beta_2\in\Delta_1(\alpha)$. 因此 k^x 交换 $\Delta_1(\beta_1)-\{\alpha\}$ 和 $\Delta_1(\beta_2)-\{\alpha\}$. 故 k 是 3 个对换的乘积. 这样一来 $|K|=2$. 于是 $|G|=60$ 或 120. 而当 $|G|=120$ 时 G 中有奇置换，所以 G 中全部偶置换组成一个正规子群 H. 注意此时 H 中 2 阶元是 4 个对换的乘积，而 3 阶元只有一个不动点. 于是 H_α 的轨道长度仍为 $1,3,6$. 因此 H 为本原群.

总之我们得到了一个 60 阶本原群 H. (当 $|G|=60$ 时 $G=H$, 否则 $|G:H|=2$).

由于 $|H_\alpha|\not\equiv 0(\text{mod }5)$, H 中 5 阶元素为两个 5 轮换的乘积. H 中 Sylow 5-子群的个数 $n_5=1$ 或 6. 若 $n_5=1$, 则 Sylow 5-子群的正规化子中有 3 阶元，因而它与 5 阶元素可交换. 这是不可能的. 因此 $n_5=6$. 现在设 $1\neq N\lhd H$, 则 N 在 Ω 上传递， N 包含全部 Sylow 5-子群. 故 $30\,\big|\,|N|$. 而 $|N|=30$ 时它有一个 15 阶正规子群. 这又是不可能的. 这就证明了 H 为单群. 因而 $H\cong A_5$. 而当 $|G:H|=2$ 时 $G\leq \text{Aut}(A_5)=S_5$, 即 $G\cong S_5$. □

例 4.18 设 T 为非交换单群， $G=T\times T$. G 中元素可以写成 (t_1,t_2), $t_i\in T$, 的形状. 取子群

$$D=\{(t_1,t_2)\,\big|\,t_1,t_2\in T,t_1=t_2\},$$

证明 D 为极大子群，因而 G 在 D 的右陪集集合 Ω 上的置换表示为本原群. 求其次级数.

解 设 $D<X\leq G$. 则 X 中有一个元素 $x=(t_1,t_2)$, $t_1\neq t_2$. 因为 $y=(t_2,t_2)\in D\leq X$, 故 X 中包含 $xy^{-1}=(t_1t_2^{-1},1)=(t,1)$, $t\neq 1$. 任取 $z=(s,s)$, $s\in T$, 则 $(t,1)^z=(t^s,1)$. 所以对 t 在 T 中任一共轭 t', $(t',1)\in X$. 但单群 T 由某一个非单位元素的全部共轭

生成. 故对一切 $t \in T$, $(t,1) \in X$. 同理知 $(1,t) \in X$, 于是 $X = G$. 所以 D 为极大子群.

由于 $|G| = |T|^2$, 而 $|D| = |T|$. 所以 $|\Omega| = |T|$. 令 $T_1 = \{(t,1) \mid t \in T\}$, $T_2 = \{(1,t) \mid t \in T\}$, 则 $G = T_1 \times T_1$, T_1, T_2 为 G 的全部极大正规子群. 由于 $T_i \cap D = \{1\}$. T_i 为正则的. 于是 D 的每个右陪集中可选取 T_1 中元素作为代表元.

取 $1 \neq s \in T$, 令 $\alpha = D$, $\beta = D(s,1)$. 则 $G_\alpha = D$, 而 $D_\beta = D^{(s,1)} \cap D$. 由于 $(t,t)^{(s,1)} = (t^s, t)$, 而 $t = t^s$ 当且仅当 s 与 t 交换, 所以

$$G_{\alpha\beta} = \{(t,t) \mid t \in C_T(s)\}$$

这证明 β 所在的次轨道长度为 $|G_\alpha : G_{\alpha\beta}| = |T : C_T(s)|$, 这正是包含 s 的共轭类的长度.

当 $T = A_5$ 时上述本原群的次级数为 1, 12, 12, 15, 20.

D 以及它的共轭称为 G *的对角子群*. □

§5. 本原群的群论结构

上一节我们建立了次轨道的概念, 并且用轨道图的方法得到了一些有用的结论. 当本原群非 2-传递且秩较小或级数 $|\Omega|$ 较小时, 这种方法是很有效的. 本节从群论结构本身讨论本原群. 在本节第一部分中讨论本原群的基柱以及它如何作用于点集 Ω 上. 第二部分中, 我们构造出一些本原群, 并且按其构造的不同, 把它们归入几种 "类型" 中. 第三部分则叙述本原群理论中的著名的 O'Nan-Scott 定理. 限于篇幅, 我们将不给出证明. 虽然如此, 第二部分的内容对我们理解这个定理会很有帮助.

§5.1 本原群的基柱

设 G 为 Ω 上本原群. 熟知所谓 G *的基柱* 是指 G 的全体极小正规子群之积, 而每个极小正规子群都是相互同构的一些单群的直积.

定理 5.1 设 G 为 Ω 上本原群， M 为 G 的一个极小正规子群，而 H 为 G 的基柱. 则下列三种情况之一成立.

(1) M 为初等交换 p-群， p 为一素数. 此时 M 为 Ω 上的正则群， $C_G(M)=M$ 且 $H=M$.

(2) M 为相互同构的非交换单群的直积， M 正则地作用于 Ω 上， $C=C_G(M)\neq 1$, C 也为 G 的极小正规子群. 此时 C 与 M 置换同构并且 $H=M\times C$.

(3) M 为相互同构的非交换单群的直积， $C_G(M)=1$, 而 $H=M$.

在一切情况下，基柱 H 是一些相互同构的单群的直积.

证　若 M 为 p 阶循环群的直积，则 M 为交换群. 由于 $M\lhd G$, M 在 Ω 上传递. 于是 M 为 Ω 上的正则群. 此时 $C_G(M)=M$, 情况 (1) 成立.

若 M 为非交换单群的直积，即 $M=T_1\times\cdots\times T_m$, $m\geq 1$, $T_i\cong T$ 为非交换单群. 此时因 $M\lhd G$, M 在 Ω 上传递. 若 $C_G(M)=1$ 成立，则 M 为 G 的唯一极小正规子群，因而 $H=M$, (3) 成立. 设 $C=C_G(M)\neq 1$. 此时 C 为半正则群. 而 $C\lhd G$, 因而 C 在 Ω 上传递. 于是 C 为正则群. 而 $M\leq C_G(C)$ 也应为半正则群，因而 M 为正则群. 因此又知 C 与 M 为同一个群的左正则表示和右正则表示，于是 C 与 M 是置换同构的. 由于 C 为正则的，所以 C 是 G 的极小正规子群. 但 G 的一切异于 M 的极小正规子群都与 M 可交换，所以 M 和 C 是 G 的全部极小正规子群. 因此 $H=C\times M$. (2) 成立. □

注意在定理 5.1 情况 (3) 中极小正规子群可能是正则群也可能是非正则群.

显然，若 H 为 G 的基柱，则 $G\leq N_{S_\Omega}(H)$. H 作为 Ω 上的置换群，它的正规化子 $N_{S_\Omega}(H)$ 与 H 如何作用于 Ω 上有关. 因此我们需要较为详细地讨论 H 在 Ω 上的作用. 这等价于讨论 H 的点稳定子群 H_α, 其中 $\alpha\in\Omega$. 以下假设 $H_\alpha\neq 1$, 故 $H=T_1\times\cdots\times T_m$ 为非交换单群的直积.

我们用 $(t_1,\cdots,t_m)$, $t_i\in T$, 来表示 H 中的元素. 此时

$$T_i=\{(t_1,\cdots,t_i,\cdots,t_m)\mid t_i\in T,\ 而\ t_j=1,\ \forall j\neq i\}.$$

定义 H 到 T_i 的映射

$$\pi_i:(t_1,\cdots,t_i,\cdots,t_m)\mapsto(1,\cdots,1,t_i,1,\cdots,1).$$

显见 π_i 是 H 到 T_i 上的同态. 把 π_i 称为 H 到 T_i 的射影. H 的某元素或某子群在 π_i 下的像也称该元素或子群在 T_i 上的射影.

在以下的讨论中, 有些事实常常用到. 我们将其写成引理.

引理 5.2 *当 $\alpha\in\Omega$ 时 H_α 为 H 中极大的 G_α-不变的子群.*

这由 G 的本原性, 即 G_α 为 G 的极大子群的事实推出.

令 $S=\{T_1,T_2\cdots,T_m\}$, $\Gamma=\{1,2,\cdots,m\}$. 则 $T_1,\cdots,T_m$ 为 H 的全部极小正规子群. 若 $x\in G$, 则 $T_i^x=T_j$ 对某个 $j\in\Gamma$. 故 x 诱导出 S 的, 因而 Γ 的一个置换. 进而 G 作用于 S 和 Γ 上.

引理 5.3 *我们可以假设 G 传递地作用于 S 上和 Γ 上.*

证 若 H 本身为 G 的极小正规子群, 这是显然的. 今设 $H=M\times C$(即定理 5.2 中情况 (2)). 此时 M 和 C 是置换同构的. 于是有 $g\in S_\Omega$, 使 $M^g=C$. 注意 $C=C_{S_\Omega}(M)$, 故 $C^g=C_{S_\Omega}(M^g)=C_{S_\Omega}(C)=M$. 所以 $C^g=M$. 这说明 $H^g=H$. 把 g 添加到 G 上得 $G_1=\langle G,g\rangle$. 此时 H 仍为 G_1 的基柱, 但 H 又是 G_1 的唯一极小正规子群, 因而 G_1 传递地作用于 S 上. 易知用 G_1 代替 G, H 以及它在 Ω 上的作用不变. □

引理 5.4 *G 和 G_α 在 S 上的作用有相同的像. 特别 G_α 在 S 上的作用传递.*

实际上, 由于 H 在 Ω 上传递, $H=HG_\alpha$. 但 H 平凡地作用于 S 上. □

考虑 π_i 在 H_α 上的作用.

引理 5.5 若 $x \in G_\alpha$, 且 $T_i^x = T_j$, 则 $\pi_i(H_\alpha)^x = \pi_j(H_\alpha)$.

证 设 $h \in H$, 我们也可写 $h = t_1 t_2 \cdots t_m$, 其中 $t_i \in T_i$. 此时 $\pi_i(h) = t_i$. 但 $h^x = t_1^x \cdots t_i^x \cdots t_m^x$. 在这个展开式中仅有 $t_i^x \in T_j$. 所以 $\pi_j(h^x) = t_i^x = \pi_i(h)^x$. 由于 $x \in G_\alpha$ 时 $H_\alpha^x = H_\alpha$, 引理成立. □

由引理知, 若又有 $y \in G_\alpha$, 且 $T_i^y = T_j$, 则 $\pi_i(H_\alpha)^x = \pi_i(H_\alpha)^y$. 又由于 G_α 在 S 上是传递的, 所以 $\pi_1(H_\alpha) = 1$ 时 $\pi_j(H_\alpha) = 1$ $\forall j \in \Gamma$. 因此 $H_\alpha \neq 1$ 时 $\pi_1(H_\alpha) \neq 1$.

下面的命题讨论 $1 \neq \pi_1(H_\alpha) \neq T_1$ 的情况, 取 $x_1, \cdots, x_m \in G_\alpha$ 使 $T_1^{x_i} = T_i$. 由引理 5.4, 这样的 $x_1, \cdots, x_m$ 是存在的.

命题 5.6 设 $1 \neq \pi_1(H_\alpha) = R_1 < T_1$. 令 $R_i = R_1^{x_i}$. 则 $H_\alpha = R_1 \times \cdots \times R_m$.

证 由引理 5.5, $R_i = R_1^{x_i} = \pi_1(H_\alpha)^{x_i} = \pi_i(H_\alpha)$. 集合 $\{R_1, \cdots, R_m\}$ 是 G_α-不变的. 实际上, 若 $y \in G_\alpha$ 且 $T_i^y = T_j$, 则由引理 5.5, $R_i^y = \pi_i(H_\alpha)^y = \pi_j(H_\alpha) = R_j$. 令 $X = R_1 \times \cdots \times R_m$. 则 X 是 H 中 G_α-不变的真子群. 由引理 5.2, $X \leq H_\alpha$. 但 X 是 H 的满足条件 $\pi_i(X) = R_i, \forall i \in \Gamma$ 的最大的子群. 因此 $H_\alpha = X$. □

下面转而讨论 $\pi_1(H_\alpha) = T_1$ 的情况. 首先, 下面的集合

$$D = \{(t, t, \cdots, t) \mid t \in T\} \tag{5.1}$$

是 H 的子群. 我们仍称它为 H 的对角子群. 若 $\Gamma = \{1, 2, \cdots, m\} = \Gamma_1 \cup \cdots \cup \Gamma_k$, 其中 $\Gamma_i \cap \Gamma_j = \varnothing, \forall i \neq j$. 令

$$D_i = \{(t_1, \cdots, t_m) \mid t_u = 1 \text{ 若} u \notin \Gamma_i, t_u = t_s\ \forall u, s \in \Gamma_i\} \tag{5.2}$$

则对每个 $i \in \{1, 2, \cdots, k\}$, D_i 为 $\prod\limits_{j \in \Gamma_i} T_j$ 的对角子群.

命题 5.7 *若 $\pi_1(H_\alpha) = T_1$, 则在适当改变 $T_1, \cdots, T_m$ 中元素的名称后, H_α 有两种可能:*

(1) $H_\alpha = D$;

(2) $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_k$, 其中 $\Gamma_i \cap \Gamma_j = \varnothing$ 且 $|\Gamma_i| = |\Gamma_j|, \forall i, j$. 而 $H_\alpha = D_1 \times \cdots \times D_k$, D_i 为 $\prod_{j \in \Gamma_i} T_j$ 的对角子群.

证 由 $\pi_1(H_a) = T_1$ 可推出 $\pi_i(H_a) = T_i \ \forall i \in \Gamma$. 考虑射影 π_i 在 H_α 上的限制 $\pi_i|_{H_\alpha}$ 的核. 易知它由 H_α 中那些"第 i 个分量"为 1 的元素组成.

在 Γ 上定义关系"$\sim$": $i \sim j$ 当且仅当 $\pi_i|_{H_\alpha}$ 的核等于 $\pi_j|_{H_\alpha}$ 的核. 这显然是一个等价关系. 于是 Γ 可以写成在关系 $\sim$ 下的等价类之并: $\Gamma = \Gamma_1 \cup \cdots \Gamma_k$. 我们断言关系"$\sim$"是在 G_α 下不变的. 实际上, 若 $i \sim j$, 则对 $h \in H_\alpha$, $\pi_i(h) = 1$ 当且仅当 $\pi_j(h) = 1$. 而若 $x \in G$, $T_i^x = T_s$, $T_j^x = T_u$. 则 $\pi_i(h)^x = \pi_s(h^x)$, $\pi_j(h)^x = \pi_u(h^x)$. 所以 $\pi_s(h) = 1$ 当且仅当 $\pi_u(h) = 1$. 故而 $s \sim u$. 而 G_α 在 S 上, 因而在 Γ 上传递, 这推出 $|\Gamma_1| = \cdots = |\Gamma_k| = l$, 此时有 $m = kl$. 重新排列 Γ 中元素, 可设 $\Gamma_1 = \{1, 2, \cdots, l\}$, $\Gamma_2 = \{l+1, \cdots, 2l\}, \cdots$. 设 $i \sim j$, 则对 $h, h' \in H_\alpha$, 只要 $\pi_i(h) = \pi_i(h')$, 则又有 $\pi_j(h) = \pi_j(h')$. 因此 $\pi_i(h) \mapsto \pi_j(h)$ $(h \in H_\alpha)$ 实际上给出了 T_i 到 T_j 上的一个同构. 在每个等价类 Γ_u 中选定一个 i, 对 Γ_u 中的任一 j. 重新命名 T_j 中元素: 若 T_j 中一个元素在此同构下为 $t_i \in T_i$ 的像, 则也称该元素为 t_i. 此时 H_α 中元素有下列形状:

$$(\underbrace{t_1, \cdots, t_1}_{l}, \underbrace{t_2, \cdots, t_2}_{l}, \cdots, \underbrace{t_k, \cdots, t_k}_{l}). \tag{5.3}$$

特别当 $\Gamma = \Gamma_1$ 时

$$H_\alpha = \{(t, t, \cdots, t) \mid t \in T\}.$$

即 (1) 成立. 若 $\Gamma \neq \Gamma_1$, 则 $H_\alpha \leq D_1 \times D_2 \times \cdots \times D_k$, 其中 D_i 由 (5.2) 式表示. 由于 $D_1 \times \cdots \times D_k$ 是 G_α-不变的. 因此 $H_\alpha = D_1 \times \cdots \times D_k$. 情况 (2) 成立. □

以上的讨论处理的是基柱 H 非正则, 因而也非交换的情况. 在总结这些讨论并考虑到 H 正则的情况, 我们得到下面的定理.

定理 5.8 设 G 为 Ω 上本原群, H 为 G 的基柱. 取定 $\alpha \in \Omega$, 则 H 以及 H_α 总共有下列几种可能.

a) H 为初等交换群;

b) H 为一非交换单群;

c) $H = T_1 \times \cdots \times T_m$ 为 m 个 $(m \geq 2)$ 相互同构的非交换单群的直积, $H_\alpha = R_1 \times \cdots \times R_m$, 其中 R_i 为 T_i 的非平凡真子群, $R_1 \cong R_2 \cong \cdots \cong R_m$;

d) H 同 c), H_α 为 H 的对角子群;

e) H 同 c), Γ 有分划 $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_k$, $|\Gamma_i| = |\Gamma_j|\ \forall i, j$, $H_\alpha = D_1 \times \cdots \times D_k$, 其中 D_i 为 $\prod\limits_{j \in \Gamma_i} T_j$ 的对角子群;

f) H 同 c), 但 $H_\alpha = 1$.

注: 1. 这里除去 a),b) 以外, H 都是至少两个非交换单群的直积.

2. 显然上述某些情况可以统一, 如 a), f) 可以统一成 $H_\alpha = 1$ 的情况; b) 可视为 c), f) 中 $m = 1$ 的特殊情形; 而 d) 可作为 $k = 1$ 的情形包含在 e) 中, 但是我们这里情况的区分与本原群的类型有直接的联系.

3. 在定理的各种情况中, Ω 的长度可以明确给出. 如在 a) 中 $|\Omega| = p^a$, 其中 p 为素数, $a \geq 1$. 在 c) 中, 若 $|T_1 : R_1| = d$, 则 $|\Omega| = d^m$. 在 d) 中, $|\Omega| = |T|^{m-1}$. 在 e) 中, $|\Omega| = |T|^{m-k}$, 而在 f) 中, $|\Omega| = |T|^m$.

4. 在基柱 H 为两个极小正规子群 M, C 的直积时, 依 M 为非交换单群与否, H, H_α 属于情况 d) 或 e).

§5.2 本原群的几种类型

在这一部分, 我们将构造出一些本原群, 并且给某些群的类型规定一个名称. 这一方面说明定理 5.8 中的各种情况都有例子, 同时便于陈述以至理解 O'Nan-Scott 定理.

一. 仿射型本原群. 具有初等交换的基柱的本原群称为*仿射型本原群*.

设 G 为 Ω 上的本原群并属于仿射型. 那么基柱 $H \cong Z_p^a$. 取定 α, 把 H 元素与 Ω 上的点等同起来, 并视 H 为 $GF(p)$ 上 a 维向量空间, 则 G_α 为 $GL(a,p)$ 的子群. G 本原当且仅当 G_α 为不可约的. 此时 G 可视为 $AGL(a,p)$ 的子群.

二. 几乎单型本原群. 若 Ω 上本原群 G 的基柱 $H \cong T$ 为非交换单群, 则称 G 为几乎单型的. 此时由于 $C_G(H) = 1$, G 同构于 $\mathrm{Aut}(T)$ 的子群. 于是有 $T \lhd G \leq \mathrm{Aut}(T)$. 此时我们可以证明 T 在 Ω 上不可能正则 (这要用到 Schreier 猜想). 反过来设有几乎单群 $G : T \lhd G \leq \mathrm{Aut}(T)$. 在 G 内取一个不包含 T 的极大子群 K, G 在 K 的右陪集上的置换表示, 就给出了几乎单型本原群. 易证上边所说的表示是忠实的.

三. 乘积型本原群.

为定义乘积型本原群, 先介绍圈积的乘积作用. (关于圈积的概念可参看上册第 III 章 §5, 但这里使用的符号与前面略有不同.)

设 Δ, Γ 为两个有限集, 其中 $\Gamma = \{1,2,\cdots,m\}$. 设 A, B 分别为 Δ, Γ 上的置换群. 则圈积 $A \,\mathrm{wr}_\Gamma\, B$ 是 A^m 和 B 的半直积. $b \in B$ 在 A^m 上的作用为

$$(a_1, a_2, \cdots, a_m)^b = (a_{1^{b^{-1}}}, a_{2^{b^{-1}}}, \cdots, a_{m^{b^{-1}}}). \tag{5.4}$$

其中 $(a_1, a_2, \cdots, a_m) \in A^m$. 把 $A \,\mathrm{wr}_\Gamma\, B$ 中元素表成为 $(a_1, a_2, \cdots, a_m; b)$, 则乘法按下面的规则进行:

$$\begin{aligned}&(a_1, a_2, \cdots, a_m; b)(a_1', \cdots, a_m'; b')\\ &= (a_1 a_{1^b}', \cdots, a_m a_{m^b}'; bb')\end{aligned} \tag{5.5}$$

本节上册中讨论过 $A \,\mathrm{wr}_\Gamma\, B$(那里写作 $A \wr B$) 在积集合 $\Delta \times \Gamma$ 上的作用, 由此得到了 $\Delta \times \Gamma$ 上的非本原群. 现在考虑 $A \,\mathrm{wr}_\Gamma\, B$ 在幂集合 Δ^m 上的作用. Δ^m 中的元素可以写成 $(\delta_1, \delta_2, \cdots, \delta_m)$ 的形式, 其中 $\delta_i \in \Delta$, 各 δ_i 不一定不同. 于是 $|\Delta^m| = |\Delta|^m$. 规定

$$(\delta_1, \delta_2, \cdots, \delta_m)^{(a_1, a_2, \cdots, a_m; b)}$$

$$=(\delta_{1^{b^{-1}}}^{a_{1^{b^{-1}}}},\delta_{2^{b^{-1}}}^{a_{2^{b^{-1}}}},\cdots,\delta_{m^{b^{-1}}}^{a_{m^{b^{-1}}}}) \tag{5.6}$$

换句话说，为了得到 $(\delta_1,\delta_2,\cdots,\delta_m)$ 在 $(a_1,a_2,\cdots,a_m;b)$ 作用后的像，只要把 $(\delta_1,\delta_2,\cdots,\delta_m)$ 的第 i 个分量 δ_i 在 a_i 作用下的像 $\delta_i^{a_i}$ 送到第 i^b 个位置上去就行了. 若继续施行由元素 $(a_1',a_2',\cdots,a_m';b')$ 决定的映射，且设 $i^b=j$, $j^{b'}=k$, 则再把 $(\delta_i^{a_i})^{a_j'}$ 送到第 k 个位置上. 根据 (5.5), 以及 $(\delta_i^{a_i})^{a_j'}=\delta_i^{a_ia_j'}$, 知连续施行由 $(a_1,a_2,\cdots,a_m;b)$ 以及由 $(a_1',a_2',\cdots,a_m';b')$ 通过 (5.6) 式所规定的映射，正好等价于施行它们的乘积通过 (5.6) 式所规定的映射. 这说明 (5.6) 式确实定义了圈积 $A\ \mathrm{wr}_\Gamma B$ 在 Δ^k 上的作用. 容易看出，这个作用是忠实的，称为 $A\ \mathrm{wr}_\Gamma B$ 的乘积作用.

例 5.9 设 $\Delta=\{a,b,c\}$, $\Gamma=\{x,y\}$, $A=S_\Delta$, $B=S_\Gamma$. 则 $|\Delta\times\Gamma|=6$, $\Delta\times\Gamma$ 中元素形如 (δ,γ), 其中 $\delta\in\Delta$, $\gamma\in\Gamma$. 把 (a,x), (b,x), (c,x) 分别称为 α, β, ε. 把 (a,y), (b,y), (c,y) 分别称为 ξ, η, ζ. 则 $\Sigma=\Delta\times\Gamma=\{\alpha,\beta,\varepsilon,\xi,\eta,\zeta\}$. 令 $G=A\ \mathrm{wr}_\Gamma B$, 则 G 在 Σ 上作用的像由置换

$$(\alpha\ \beta\ \varepsilon),(\beta\ \varepsilon),(\alpha\ \xi)(\beta\ \eta)(\varepsilon\ \zeta)$$

生成. G 在 Σ 上为非本原群. 令 $\Omega=\Delta^2$, 并使用下列记号:

$$(\alpha\ \alpha)=1,\ \ (\alpha\ \beta)=2,\ \ (\alpha\ \varepsilon)=3,$$

$$(\beta\ \alpha)=4,\ \ (\beta\ \beta)=5,\ \ (\beta\ \varepsilon)=6,$$

$$(\varepsilon\ \alpha)=7,\ \ (\varepsilon\ \beta)=8,\ \ (\varepsilon\ \varepsilon)=9.$$

则 G 在 Ω 上的像由置换

$$(1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)\ \ (4\ 7)(5\ 8)(6\ 9)\ \ (2\ 4)(3\ 7)(6\ 8)$$

生成. 容易验证作为 Ω 上的置换群，G 为本原群.

定理 5.10 设 A 为集合 Δ 上置换群，B 为 Γ 上的置换群. $G=A\ \mathrm{wr}_\Gamma B$, $|\Gamma|=m$, $\Omega=\Delta^m$. G 在 Ω 上的乘积作用是本原的当且仅当 A 在 Δ 上本原，非正则且 B 在 Γ 上传递.

证 先证条件的必要性. 若 A 在 Δ 上不传递, 而 $\Delta' \subsetneqq \Delta$ 为 A 的轨道, 则 Δ^m 的真子集

$$\{(\delta_1, \delta_2, \cdots, \delta_m) \mid \delta_i \in \Delta',\ \forall i \in \Gamma\}$$

在 G 的作用下不变, 故 G 在 Ω 上不传递. 若 A 在 Δ 上传递但非本原, $\delta \in \Delta$, 则有子群 A_1 使 $A_\delta < A_1 < A$. 由 (5.5) 知

$$\{(a_1, a_2, \cdots, a_m; b) \mid a_i \in A_1, b \in B\}$$

为 G 的真子群, 并且真包含 $(\delta, \delta, \cdots, \delta) \in \Omega$ 在 G 中的稳定子群

$$\{(a_1, a_2, \cdots, a_m; b) \mid a_i \in A_\delta, b \in B\}.$$

于是 G 在 Ω 上非本原. 若 A 在 Δ 上正则, 那么取 $\alpha = (\delta, \delta, \cdots, \delta) \in \Omega$,

$$G_\alpha = \{(1, 1, \cdots, 1; b) \mid b \in B\},$$

而它真包含在子群 $\{(a, a, \cdots, a; b) \mid a \in A, b \in B\}$ 内. 故 G 在 Ω 上也是非本原的. 最后若 B 在 Γ 上不传递, 而 Γ_1 为 B 在 Γ 上的一个轨道. 则

$$\{(a_1, a_2, \cdots, a_m; b) \mid a_i \in A_\delta,\ \forall i \in \Gamma_1\}$$

为 G 的真子群同时真包含 $(\delta, \delta, \cdots, \delta)$ 的稳定子群. 故 G 在 Ω 上非本原.

再证条件的充分性. 为此记

$$X = \{(a_1, \cdots, a_m; 1) \mid a_i \in A\},$$

$$Y = \{(1, \cdots, 1; b) \mid b \in B\}.$$

于是 $X \cong A^m$, 而

$$A_i = \{(1, \cdots, 1, a_i, 1, \cdots, 1; 1) \mid a_i \in A\}$$

为 X 的正规子群. 显然 $Y \cong B$, $G = X \rtimes Y$. 首先由于 B 在 Γ 上传递. 所以对任何 i, j 都有 $y \in Y$, 使 $A_i^y = A_j$.

取定 $\alpha = (\delta, \delta, \cdots, \delta) \in \Omega$. 因为 A 在 Δ 上传递, 所以对任何 $\delta_1, \cdots, \delta_m$, 存在 a_i 使 $\delta^{a_i} = \delta_i$. 这说明对 $\beta = (\delta_1, \delta_2, \cdots, \delta_m)$, $\alpha^{(a_1, a_2, \cdots, a_m; 1)} = \beta$. 所以 X 在 Ω 上传递, 因此 G 在 Ω 上传递. 而 α 在 X 内的稳定子群为 $X_\alpha = \{(a_1, a_2, \cdots, a_m; 1) \mid a_i \in A_\delta\}$. 我们来证若有 X 的子群 Z, 使 $X_\alpha < Z$, 且 Z 是 Y-不变的, 则 $Z = X$. 设 $X_\alpha < Z$. 则有一元素 $z \in Z \backslash X_\alpha$, 这说明若 $z = (a_1, \cdots, a_m; 1)$, 则至少有一个 $a_i \notin A_\delta$. 因 A 在 Δ 上本原且非正则, $N_A(A_\delta) = A_\delta$. 这样一来有元素 $u \in A_\delta$, 但 $u^{a_i} \notin A_\delta$. 显然元素 $x = (1, \cdots, 1, \underset{i}{u}, 1, \cdots, 1) \in X_\alpha$ 但 $x^z = (1, \cdots, 1, u^{a_i}, 1, \cdots, 1) \in Z \backslash X_\alpha$. 因为 A_δ 为 A 的极大子群, 所以 $\langle A_\delta, u^{a_i} \rangle = A$, 相应地 $\langle (A_i)_\delta, x^z \rangle = A_i$. 于是 $A_i \leq Z$. 因为 Y 传递地作用 $\{A_1, \cdots, A_m\}$ 上, 所以 $A_1, A_2, \cdots, A_m \leq Z$, 即 $Z = X$. 因 $G_\alpha \geq Y$, 所以 X_α 是 X 中极大的 G_α-不变的子群. 所以 G 在 Ω 上本原. □

从这个定理可以看出, 从 Δ 上的非正则本原群 A 出发, 对 Γ 上传递群 B, 通过圈积 $G = A \operatorname{wr}_\Gamma B$ 的乘积作用, 我们可得到一个新的本原群. 若 A 为几乎单型的, 即 $T \trianglelefteq A \leq \operatorname{Aut}(T)$ 对某非交换单群, 那么 $G = A \operatorname{wr}_\Gamma B$ 的基柱 H 为 T^m, 而 $\alpha = (\delta, \delta, \cdots, \delta)$ 时, $H_\alpha = R_1 \times \cdots \times R_m$, 其中 $R_i \cong R$ 为 δ 在 T 内的稳定子群. 如果 A 为下面要介绍的对角型本原群, 则 G 为一个本原群. 以后会看到此时 G 的基柱 H 内的稳定子群 H_α 属于定理 5.8 的情况 e). 当 A 为 Δ 上几乎单型或对角型本原群时, 作用于 $\Omega = \Delta^m$ 上的本原群 $G = A \operatorname{wr}_\Gamma B$ 称为 **乘积型本原群**.

四. 对角型本原群

设 T 为非交换单群. 令 $H \cong T^m, m \geq 2$. 于是 H 中元素可以写成 $(t_1, t_2, \cdots, t_m)$ 的形状, 其中 $t_i \in T$. 令

$$D = \{(t, t, \cdots, t) \mid t \in T\},$$

则 D 为 H 的对角子群. 把 D 在 H 中的全体右陪集所成的集合记作 Ω, 则 $|\Omega| = |T|^{m-1}$, 并且 H 忠实地作用在 Ω 上. 从上节例 4.18

我们看到，若 $m=2$, H 本身就是 Ω 上本原群. 在一般情形， H 在 Ω 上传递. 用 $\alpha\in\Omega$ 表示陪集 D. 则 $H_\alpha=D$.

令 $W=N_{S_\Omega}(H)$. 由于 $H_\alpha\neq 1$, $C_W(H)=1$. 所以 W 是 H 的自同构群 $\mathrm{Aut}(H)$ 的一个子群.

命题 5.11 若 $H\cong T^m$, 其中 T 为非交换单群. 则 $\mathrm{Aut}(H)=A\,\mathrm{wr}_\Gamma\,S_\Gamma$, 其中 $A=\mathrm{Aut}(T)$, 而 $\Gamma=\{1,2,\cdots,m\}$.

证明请读者给出.

下面要弄清楚 $\mathrm{Aut}(H)$ 中怎样的元素可以出现在 W 中，以及 W 中怎样的子群是 Ω 上的本原群. 此时 $\mathrm{Aut}(H)$ 中元素可以写成

$$(a_1,\cdots,a_m;b)$$

的形状，其中 $a_i\in\mathrm{Aut}(T)$, 而 $b\in S_\Gamma$. $A=\mathrm{Aut}(T)$ 中所有 T 的内自同构组成一正规子群 $\mathrm{Inn}T$, 我们把它与 T 等同起来. 于是 H 可以嵌入到 $\mathrm{Aut}(H)$ 中. 此时 H 中元素可以写成

$$(a_1,a_2,\cdots,a_m;1),\quad a_i\in T,$$

的形状. 设 $x,y\in A$, 我们用 $x\equiv y(\mathrm{mod}\ T)$ 表示 $xy^{-1}\in T$, 即在商群 A/T 中， $xT=yT$.

定理 5.12 设 T 为非交换单群， $H\cong T^m$, $D=\{(t,\cdots,t;1)\}$, 为 H 中对角子群， Ω 表示 D 在 H 内的右陪集组成的集合, $\Gamma=\{1,2,\cdots,m\}$. 则有

(1) $W=N_{S_\Omega}(H)$ 由 $A\,\mathrm{wr}_\Gamma\,S_\Gamma$ 中形如

$$(a_1,a_2,\cdots,a_m;b),\ \text{其中}\ a_i\equiv a_j(\mathrm{mod}\ T),\ b\in S_\Gamma,\tag{5.7}$$

的元素组成.

(2) 若 $H\leq G\leq W$, 则 G 为本原群当且仅当下列两条之一成立:

(2.1) $m=2$;

(2.2) G 在 S_Γ 上的射影是 Γ 上的本原群. 此处 G 在 S_Γ 上的射影映射由 $(a_1,\cdots,a_m;b)\mapsto b$ 给出.

证 (1) 先证 W 中元素有 (5.7) 的形状. W 传递地作用于 Ω 上. 取 $\alpha = D\cdot 1$, 则 $H_\alpha = D \lhd W_\alpha$. 若 $x = (a_1, \cdots, a_m; b) \in W_\alpha$, 则 $D^x = D$. 这说明对任意的 $t \in T$,

$$(t, t, \cdots, t; 1)^x$$

仍为形如 $(t', t', \cdots, t'; 1)$ 的元素. 因此若 $i, j \in \Gamma$, 则 $t^{a_i} = t^{a_j}$ 即 $t^{a_i a_j^{-1}} = t$ 对一切 $t \in T$ 成立. 这推出 $a_i = a_j\ \forall i, j \in \Gamma$. 故 W_α 由形如 $(a, \cdots, a; b)$, $a \in A$, 的元素组成. 由于 $W = HW_\alpha$, 所以 W 中元素形如

$$(t_1 a, t_2 a, \cdots, t_m a; b), t_i \in T, a \in A, b \in S_\Gamma.$$

这正是 (5.7) 的形状.

再证一切具形状 (5.7) 的元素组成一个群 W_1, 且 $W_1 = W$. 由于

$$(a_1, \cdots, a_m; b)(a'_1, \cdots, a'_m; b') = (a_1 a'_{1^b}, \cdots, a_m a'_{m^b}; bb'),$$

容易验证若上式左边两元素具形状 (5.7), 其乘积也具形状 (5.7). 所以它们确组成一个群 W_1. 上边已证 $W \subseteq W_1$. 在 W_1 中集合

$$D_1 = \{(a, \cdots, a; b) \mid a \in A, b \in S_\Gamma\}$$

构成一个子群. 把 D_1 在 W_1 中右陪集的集合记为 Ω_1, 则 W_1 为 Ω_1 上的置换群. 而作为 Ω_1 中的"点"$D_1\cdot 1$(记作 α') 的稳定子群就是 D_1. $W_1 \supseteq H$, 但 $D_1 \cap H = D$. 故 H 在 Ω 上的表示与 H 在 Ω' 上的表示是等价的. 于是 W_1 可嵌入到 S_Ω 内, 因而 $W_1 \le N_{S_\Omega}(H) = W$. 由于 $W \subseteq W_1$, 得 $W_1 = W$. (1) 得证.

(2) $m = 2$ 的情况已经解决. 今设 $m \ge 3$.

设 $H \le G \le W$, G 是 Ω 上本原群. 仍使用上边的记号, 特别 $\alpha \in \Omega$, $W_\alpha = D_1$, 因而 $H_\alpha = D$, $G_\alpha = D_1 \cap G$. 由于 H 传递, 故 $G = HG_\alpha$. 但 W 到 S_Γ 上的射影是同态, 故 W 作用于 Γ 上. 且 H 在此作用的核内. 这样一来 G 在 Γ 上的作用与 G_α 在 Γ 上的作

用有相同的像. 如果 G 在 S_Γ 上的射影不传递, 而 $\Gamma_1 = \{1, \cdots, l\}$, $l < m$ 为一个轨道. 那么

$$Z = \{(\underbrace{t_1, \cdots, t_1}_{l}, t_2, \cdots, t_2; 1) \mid t_1, t_2 \in T\}$$

是 G_α 不变的. 但 $D < Z < H$, 与 G 在 Ω 上本原矛盾. 若 G 在 S_Γ 上的射影有非本原系 $\{\Gamma_1, \Gamma_2, \cdots, \Gamma_k\}$. 其中 $|\Gamma_i| = l > 1$, $k > 1$, 则重新排列 Γ 中元素可设 $\Gamma_1 = \{1, \cdots, l\}$, $\Gamma = \{l+1, \cdots, 2l\}$, $\cdots$. 令

$$Z = \{(\underbrace{t_1, \cdots, t_1}_{l}, \underbrace{t_2, \cdots, t_2}_{l}, \cdots, \underbrace{t_k, \cdots, t_k}_{l}; 1) \mid t_i \in T\}.$$

则又有 $D < Z < H$ 且 Z 为 G_α-不变的. 因而也是不可能的. 故 G 在 S_Γ 上的射影在 Γ 上本原.

反过来, 设 G 在 S_Γ 上的射影为 Γ 上本原群, 而 $D \le X \le H$, X 为 G_α-不变的的子群, 考察 $\pi_i|_X$ 的核并在 Γ 上定义关系 "$\sim$": $i \sim j$ 当且仅当 $\pi_i|_X$ 与 $\pi_j|_X$ 有相同的核. 那么关系 $\sim$ 的等价类就是 G_α 同时也是 G 在 S_Γ 上的射影的非本原块. 由于该射影的本原性, 要么每个等价类由一个元素组成, 要么 Γ 中元素属于一个等价类. 在前一种情况下得 $X = H$. 后一种情况下 $X = D$, 与假设矛盾. 这就完成了证明. □

定理 5.12 所描述的本原群 G 称为 *对角型本原群*. 对角型本原群的基柱及其稳定子群属于定理 5.8 的情况 d). 若 A 为集合 Δ 上的对角型本原群, B 为 Γ 上的本原群, 则 $G = A \operatorname{wr}_\Gamma B$ 通过乘积作用产生一个乘积型本原群. 此时基柱在 Ω 上的作用由定理 5.8 的情况 e) 所描述.

五. 挠圈积型本原群

挠圈积 是圈积的推广.

设 A, B, C 为三个有限群, 且 $C < B$, 并有一个 C 到 $\mathrm{Aut}(A)$ 的同态 φ. 设 $|B : C| = m > 1$, 而 $y_1, y_2, \cdots, y_m$ 为 C 在 B 内的右陪集代表. 再令 $\Gamma = \{1, 2, \cdots, m\}$. 此时我们来构造一个新的群.

首先令 $X = A^m$. X 中元素记作 $(a_1, a_2, \cdots, a_m)$, $a_i \in A$. 再定义 B 在 X 上的作用. 对 $b \in B$, 则 $y_i b$ 在某陪集 Cy_j 内. 于是 b 引起了 Γ 上的置换 $i^b = j$. 并且有 $c_i \in C$, 使 $y_i b = c_i y_j$. 由 b 定义 X 到自身的映射

$$\tilde{b}: (a_1, \cdots, a_m) \mapsto (a'_1, \cdots, a'_m), \tag{5.8}$$

其中 $a'_j = a_i^{\varphi(c_i)}$. 因为 φ 是 C 到 $\mathrm{Aut}(A)$ 的同态, 易证 $\tilde{b}$ 是 X 的自同构. 进而若又有 $b' \in B$, $y_j b' = c'_j y_k$. 那么按 (5.8), 且

$$\widetilde{b'}: (a'_1, \cdots, a'_m) \mapsto (a''_1, \cdots, a''_m)$$

时, $a''_k = (a'_j)^{\varphi(c'_j)} = a_i^{\varphi(c_i c'_j)}$. 另一方面 $y_i(bb') = (c_i c_j) y_k$. 所以 $\tilde{b} \cdot \widetilde{b'} = \widetilde{bb'}$. 故 (5.8) 确实定义了 B 在 X 上的作用. 由此构造半直积 $G = X \rtimes B$, G 称为 A 与 B 关于 φ 的**挠圈积**, 记作 $G = A\ \mathrm{wr}_\varphi B$.

容易看出, 当 A 为一个群, B 为 Γ 上传递群, 取 $\gamma \in \Gamma$, $C = B_\gamma$, 而且对任意的 $c \in C$, $\varphi(c)$ 为 A 的恒等自同构, 那么挠圈积 $A\ \mathrm{wr}_\varphi B$ 就是通常的圈积 $A\ \mathrm{wr}_\Gamma B$.

设 $G = A\ \mathrm{wr}_\varphi B$ 为挠圈积, 视 B 为 G 的子群. 则得 G 关于子群 B 的传递表示. 在一定的条件下, 这个表示是忠实的. 如果 Ω 上的本原群 G 的基柱为 $H = T^m$, 其中 T 为非交换单群, 并且有子群 $B = G_\alpha \geq C$, 和同态 $\varphi: C \to \mathrm{Aut}(T)$, 使 $G = T\ \mathrm{wr}_\varphi B$, 则称 G 为**挠圈积型本原群**. 显然此时 H 在 Ω 上正则.

限于篇幅, 我们不去讨论何时能产生挠圈积型本原群. 仅用下边的例子说明这类本原群是存在的.

例 5.13 取 $A = A_5$, $B = A_6$, 且 B 作用于 $\Gamma = \{1, 2, \cdots, 6\}$ 上. 令 C 为点 6 的在 B 中的稳定子群. 于是 C 为 $\Gamma_1 = \{1, 2, \cdots, 5\}$ 上的交错群. 把 A 也看成 Γ_1 上置换群. 对 $c \in C$, $a \in A$, 规定 $a^{\varphi(c)} = c^{-1}ac$, 即 $\varphi(c)$ 为由 c 所定义的内自同构. 令 $b = (1\ 2\ 3\ 4\ 5)$, 选取陪集代表

$$y_1 = 1, y_2 = (1\ 2\ 6), y_{i+1} = y_i b \quad 2 \leq i \leq 5.$$

仍用 $(a_1, a_2, \cdots, a_6)$, $a_i \in A$, 表示 X 中元素. 则在陪集代表 $y_1, \cdots, y_t$ 下

$$(a_1, a_2, \cdots, a_6)^b = (a_1^b, a_6, a_2, a_3, a_4, a_5). \tag{5.9}$$

我们可以构造圈积 $G = A \operatorname{wr}_\varphi B$. 它的阶为 $60^6 \cdot 360$. 视 B 为 G 的子群, 由于 $C_G(X) \cap B = 1$. 所以 G 忠实地表示成一个次数为 60^6 的传递群. 再证此时 G 为本原群, 为此只需证若 $1 < Z \leq X$, 且 Z 为 B-不变的, 则 $Z = X$. 设 $1 \neq z \in Z$, 则 z 有一个分量不为 1. 用适当的 B 中元素作用可设 z 的第一个分量 $a_1 \neq 1$. 若 $c \in C$, 则 z^c 的第一个分量为 a_1^c. 当 c 跑遍 C 时, 知对 a_1 的任意共轭 a_1', Z 中有元素 z', 其第一个分量为 a_1'. 这样一来 $\pi_1(Z) = A_1$. 由于 B 本原地作用于 Γ 上. 知 $Z \neq X$ 时必为 X 的对角子群 D. 这样一来可把 G 表示成 DB 的右陪集集合上的对角型本原群. 此时, 若用 X_1 表示 X 中形如 $(a_1, 1, \cdots, 1)$, $a_1 \in A$, 的元素组成的子群, 则应有 $C \leq C_G(X_1)$. 但在我们的情况下, $C_G(X_1) = 1$. 故 $Z = D$ 是不可能的.

§5.3 O'Nan-Scott 定理

现在我们可以来叙述 O'Nan-Scott 定理了.

定理 5.14 (O'Nan-Scott) *设 $G \leq S_\Omega$ 为本原群, 则 G 必属于下述五种类型之一: 仿射型, 几乎单型, 乘积型, 对角型和挠圈积型.*

这个定理是 O'Nan 和 Scott 首先宣布的. 但当时他们漏掉了最后一个类型, 同时也未给出证明. 后来许多人, 包括 Cameron; Liebeck, Praeger 和 Saxl; Buekenhout 等人先后进行了讨论, 并给出了完全的证明. 但在不同的文章中, 类型的区分也不完全一致. 这里采用的是 Libedk, Praeger 和 Saxl 的一篇文章里的分法. 这个定理对本原群理论有基本的意义. 特别把它与有限单群分类定理结合起来, 常常可以决定本原群的确切的构造.

为证明这个定理, 我们只需在本节定理 5.8 的基础上建立下列事实: 1) 若本原群 G 的基柱为非交换单群 T, 则 $T_\alpha \neq 1$; 2) 若

H, H_α 如定理 5.8 情况 c) 或 e) 所描述, G 为乘积型; 3) 若 H, H_α 如定理 5.8 情况 d) 所描述, G 为对角型; 4) 若 H, H_α 如定理 5.8, f), 则 G 为挠圈积. 读者能够看出, 我们的定理 5.12 即是事实 3). 下面用事实 1) 的证明来结束本节. 证明要用到 Schreier 猜想.

定理 5.15 *若本原群 $G \le S_\Omega$ 的基柱 T 为非交换单群, $\alpha \in \Omega$, 则 $T_\alpha \ne 1$.*

证 此时 $C_G(T) = 1$, 所以 $G \le \mathrm{Aut}(T)$. 设 T 为正则的, 我们推出矛盾. 因 T 正则, 则 $G = TG_\alpha, T \cap G_\alpha = 1$. 于是 $G_\alpha \cong G/T$, G_α 可视为 T 的外自同构群的一个子群.

Schreier 猜想说, 每个单群的外自同构群都是可解群. 于是 G_α 可解. G_α 有一个极小正规子群 P, P 为初等交换 p-群, p 为素数.

由于 G_α 为极大子群, 且 $1 \ne P \lhd G_\alpha$, 故 $N_G(P) = G_\alpha$. 于是 $C_T(P) = 1$. 这说明在 P 的共轭作用下, T 中单位元素自身组成一个长为 1 的轨道, T 的其它元素都属于长度为 p 的倍数的轨道. 因此 $p \mid |T| - 1$, 从而 $p \nmid |T|$.

设素数 $q \mid |T|$. 令 $S = \{Q_1, \cdots, Q_l\}$ 为 T 中全部 Sylow q-子群的集合. P 共轭地作用于 S 上. 由于 $(p, |T|) = 1$ 而 $l \mid |T|$. 必有某个 Q_i 在 P 下不动. 若又有 Q_j 在 P 下不动. 那么有 $x \in T$ 使 $Q_j = Q_i^x$. 因而 Q_j 在 P^x 下也不动. 这说明 P, P^x 为 $N_{TP}(Q_j)$ 中的两个 Sylow p-子群, 因而有 $y \in N_{TP}(Q_j)$, 使 $Q_i^x = Q_j^y$. 这里 y 可写成 $y = uv, u \in P, v \in T$. 这样一来 $P^x = P^y = P^v$, 而 $xv^{-1} \in N_G(P) \cap T = 1$. 故 $x = v$. 这样有 $Q_i = Q_j$. 所以有且只有一个 Sylow q-子群 Q_i 在 P 下不动. 由于 $P \lhd G_\alpha$, Q_i 在 G_α 下不动, 这样一来 Q_iG_α 为子群且 $G_\alpha \le Q_iG_\alpha \le G$. 得到 $Q_i = T$. 矛盾. 定理得证. □

想进一步了解 O'Nan-Scott 定理的读者可参看下列文章:

P.J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13**(1981), 1–22.

M.W. Liebeck, C.E. Praeger and J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Austral. Math. Soc. Ser. A* **44**(1988), 389–396.

F. Buekenhout, On a theorem of O'Nan-Scott, *Bull. Soc. Math. Belg.*, **40**(1988), 1–9.

§6. 有较小级的传递子群的本原群

在本节我们在下列条件下讨论置换群 G 的传递性:

(1) G 在 Ω 上为本原群;

(2) $\Omega=\Delta\cup\Gamma$, $\Delta\cap\Gamma=\varnothing$, $2\leq|\Gamma|<|\Omega|$;

(3) G_Δ 在 Γ 上为传递群;

以及比 (3) 稍强的条件

(3′) G_Δ 在 Γ 上本原.

我们有下面的定理.

定理 6.1 *设 G,Ω,Δ,Γ 满足 (1), (2), (3), 则 G 在 Ω 上为 2 重传递群. 若 G,Ω,Δ,Γ 满足 (1), (2), (3′), 则 G 为 Ω 上的 2 重本原群.*

证 在 $|\Gamma|\geq\frac{1}{2}|\Omega|$ 的情况下我们立即得到结论. 取定 $\alpha\in\Omega$ 和 G_α 在 $\Omega-\{\alpha\}$ 上的一个轨道 Σ. 设 $\beta\in\Sigma$. 因 G 为本原群, 故 G 中有元素 g, 使 $\alpha\notin\Gamma^g$, 而 $\beta\in\Gamma^g$. 此时 $\alpha\in\Delta^g$, 而 $G_\alpha\geq G_{\Delta^g}$, 后者在 Γ^g 上传递. 但 $\beta\in\Gamma^g\cap\Sigma$, 所以 $\Gamma^g\subseteq\Sigma$. 这说明 $|\Sigma|>\frac{1}{2}(|\Omega|-1)$. 于是 G_α 在 $\Omega-\{\alpha\}$ 上的轨道只有一个, G_α 在 $\Omega-\{\alpha\}$ 上传递. 即 G 为 Ω 上 2 重传递群. 若 G_Δ 在 Γ 上本原, 则传递群 $G_\alpha\geq G_{\Delta^g}$, 而 G_{Δ^g} 在 Γ^g 上本原, 又由 $|\Gamma^g|=|\Gamma|>\frac{1}{2}(|\Omega|-1)$, 所以 G_α 在 $\Omega-\{\alpha\}$ 上本原. 于是当 $|\Gamma|\geq\frac{1}{2}|\Omega|$ 时定理成立.

今设 $|\Gamma|<\frac{1}{2}|\Omega|$, 我们证明此时有 Δ^*,Γ^* 使条件 (1), (2), (3) 或相应的 (1), (2), (3′) 对 Δ^*,Γ^* 成立且 $|\Gamma^*|>|\Gamma|$. 实际上因 $|\Gamma|\geq 2$, 可取 $\beta\neq\gamma\in\Gamma$. 由于 G 在 Ω 上本原, 有元素 g 使 $\beta\in\Gamma^g,\gamma\notin\Gamma^g$. 令 $\Gamma^*=\Gamma\cup\Gamma^g$, 而 $\Delta^*=\Delta\cap\Delta^g$, 显然此时 (2) 成立. $\beta\in\Gamma\cap\Gamma^g$, 所以 $G_{\Delta^*}\geq\langle G_\Delta,G_{\Delta^g}\rangle$ 在 Γ^* 上传递. 于是 Δ^*,Γ^* 也满足 (1), (2),

(3). 若对 Δ, Γ, 条件 (3′) 成立. 则 G_{Δ^*} 包含子群 G_Δ, 它在 Γ 上本原, 而因 $\beta \in \Gamma \cap \Gamma^g$, 所以 $|\Gamma| > \frac{1}{2}|\Gamma^*|$, 由推论 4.6 知 G_{Δ^*} 在 Γ^* 上也本原, 即对 Δ^*, Γ^* 条件 (3′) 也成立. 因为 $\gamma \notin \Gamma^g$, 故 $\Gamma^* \neq \Omega$, 且 $|\Gamma^*| > |\Gamma|$. 利用上述方法可将问题化成 $|\Gamma| \geq \frac{1}{2}|\Omega|$ 的情况. □

推论 6.2 *在 (1), (2), (3′) 的条件下, 若 $n = |\Omega|, k = |\Delta|$, 则 G 为 $k+1$ 重本原的.*

证 当 $k = 1$ 时这是显然的. 设结论对 $|\Delta| < k$ 已经成立. 今设 $|\Delta| = k$. 取 $\alpha \in \Delta$. 由于 G 为 2 本原的, 所以 G_α 为本原群. 于是 G_α, $\Omega - \{\alpha\}$, $\Delta - \{\alpha\}$, Γ 也满足 (1), (2), (3′). 但此时 $|\Delta - \{\alpha\}| = k - 1$, 所以 G_α 为 k 重本原群, 即 G 为 $k+1$ 重本原群. □

推论 6.3 *设 G 为 Ω 上本原群, 若 G 包含一个对换, 则 $G = S_\Omega$; 若 G 包含一个 3-轮换, 则 $G = A_\Omega$ 或 S_Ω.*

定理 6.4 *设 G 为 Ω 上本原群, $|\Omega| = n = k + p$, 其中 p 为素数而 $k \geq 3$, 若 G 包含一个 p 轮换, 则 $G \geq A_\Omega$.*

证 设 $\Omega = \{1, 2, \cdots, p, \cdots, p+k\}$, $x = (1\ 2\ \cdots\ p) \in G$. 记 $\Delta = \{p+1, \cdots, p+k\}$, $\Gamma = \{1, 2, \cdots, p\}$. 因为 $G_\Delta \geq \langle x \rangle$ 在 Γ 上本原, 由定理 6.1, G 是 $(k+1)$-本原的. 又 $P = \langle x \rangle$ 为 G_Δ 的 Sylow p-子群, 它满足定理 3.6 的条件. 于是 $N = N_G(P)$ 在 Δ 上 k-传递, 即 $N^\Delta \cong S_\Delta$. 记 $C = C_G(P)$, N/C 同构于 $\mathrm{Aut}(P)$ 的子群, 为循环群, 因此 N^Δ / C^Δ 也为循环群. 这样一来 $C^\Delta \geq A_\Delta$. 而显然 $C^\Gamma = P$. 于是 $C \geq A_\Delta \times \langle x \rangle$, C 中有一个 3-轮换. 由推论 6.3 就得到我们的结论. □

例 6.5 决定所有 6 级本原群.

解 设 G 为 6 级本原群, 作用于 $\Omega = \{1, 2, \cdots, 6\}$ 上.

可设 $G \not\geq A_\Omega$. 由于 6 级本原群总是 2-传递的, 所以 $30 \mid |G|$. 在 A_Ω 中有 36 个 Sylow 5-子群, 它们生成 A_Ω. 因此 G 中有 6

个 Sylow 5-子群. 设 P 为 G 的一个 Sylow 5-子群, 它有一个不动点 $\alpha \in \Omega$. 因此 $G_\alpha = N_G(P)$. 先设 G 中没有奇置换. 此时 $|N_G(P)| = 10$, $|G| = 60$. 易知 G 为单群. 于是有 $G \cong A_5$. 若 G 有奇置换, 则 $|N_G(P)| = 20$, $|G| = 120$, 且 $G \cap A_\Omega$ 同构于 A_5. 此时 $G \lesssim \mathrm{Aut}(A_5) = S_5$. 因而 $G \cong S_5$. 反过来, 由于 A_5, S_5 中确有 6 个 Sylow 5-子群, 这样的 6 级本原群存在.

总结以上讨论, 6 级本原群 G 只有 4 种可能: 1) $G \cong A_5$; 2) $G \cong S_5$; 3) $G \cong A_6$; 4) $G \cong S_6$. □

例 6.6 决定全部 7 级本原群

解 设 G 为 $\Omega = \{1, 2, \cdots, 7\}$ 上本原群. 仍先设 $G \not\geq A_\Omega$. 因 $7 \mid |G|$, 设 P 为 G 的一个 Sylow 7-子群. 显然 $C_{A_\Omega}(P) = P$.

情形 1. $P \trianglelefteq G$. 此时 $P = \langle x \rangle$, 其中 $x = (1\ 2\ 3\ 4\ 5\ 6\ 7)$. 取 $y = (2\ 4\ 3\ 7\ 5\ 6)$, 则 $N_{S_\Omega}(P) = \langle x, y \rangle$. 于是 G 有下列几种可能:

1.1) $G = \langle x \rangle$, $|G| = 7$;

1.2) $G = \langle x, y^3 \rangle$, $|G| = 14$;

1.3) $G = \langle x, y^2 \rangle$, $|G| = 21$;

1.4) $G = \langle x, y \rangle$, $|G| = 42$.

情形 2. $P \ntrianglelefteq G$.

先设 G 中没有奇置换. 此时 $N_G(P) = \langle x \rangle$ 或 $\langle x, y^2 \rangle$, 其中 x, y 为情形 1 中所定义的元素. 但由 Burnside 定理, $N_G(P) \neq C_G(P)$. 故 $N_G(P) = \langle x, y^2 \rangle$. 这样一来, $N_G(P) = N_{A_\Omega}(P)$, 因而 G 中 Sylow 7-子群的个数 n_7 为 A_Ω 中 Sylow 7-子群的个数 120 的因子. 所以 $n_7 = 8$ 或 15. 但 $n_7 = 15$ 导致 $9 \mid |G|$, 因而 G 有 3-轮换. 由推论 6.3 知, 这与 $G \not\geq A_\Omega$ 相违. 所以 $n_7 = 8$. 因此 $|G| = 168$. 易知此时 G 为单群, 所以 $G \cong PSL(3, 2)$. 反过来, 把 $PSL(3, 2)$ 看成 $GF(2)$ 上的 3 维向量空间 V 上的线性群, 它忠实作用于 V 中 7 个非零向量上. 于是略加计算后知此时有

2.1) $G = \langle x, y^2, z \rangle$, $|G| = 168$, 其中 $z = (3\ 5)(6\ 7)$.

若 G 有奇置换, 那么 $G \cap A_\Omega$ 为 2.1) 所示的 168 阶单群. 此时 $N_G(P) = \langle x, y \rangle$. 于是 $yz = (2\ 4\ 5\ 7\ 3\ 6)$, 而 $(yz)^2 = (2\ 5\ 3)(4\ 7\ 6)$.

这样一来，$y^2(yz)^2 = (4\ 6\ 7) \in G$. 这导致 $G \geq A_\Omega$. 这说明当 $G \ngeq A_\Omega$ 时只有 2.1) 一种可能.

总结以上讨论，知在同构的意义下，7 级本原群有 7 个，即 1.1)–1.4), 2.1) 以及 A_7 和 S_7. □

§7. Mathieu 群

上世纪六、七十年代，Mathieu 发现了五个多重传递群：M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. 它们的重要性在于，一方面，其中 M_{11}, M_{12}, M_{23}, M_{24} 是除去 $A_n, n \geq 6$, $S_n, n \geq 4$, 以外的仅有的 4 重或 4 重以上的传递群；另一方面，这 4 个群，以及 M_{22} 的导群是最早发现的"零散单群". 人们对这五个群进行了充分的研究. 本节介绍 M_{11}, M_{12} 这两个小 Mathieu 群的最基本的理论.

定义 7.1 设 H 为集合 Ω 上的置换群. $*$ 为 Ω 外的一个符号. 令 $\Omega^* = \{*\} \cup \Omega$. 若 G 是 Ω^* 上的传递群，且 $*$ 在 G 中的稳定子群正好是 H(它也看成 Ω^* 上的置换群), 则称 G 为 H 的传递扩张.

显然，若 G 是事先给定的 Ω^* 上的传递群，那么 G 是 G_* 的传递扩张. 反过来，若 H 已给定，在什么条件下它有传递扩张以及如何构造出来，是一个不容易解决的问题. 但在某些特殊情况，我们可以得到传递扩张.

定理 7.2 *设 H 为 Ω 上一个 2 重传递群. $\alpha \in \Omega$, $\Omega^* = \{*\} \cup \Omega$. 设 S_{Ω^*} 中有元素 x, H 中有元素 y 满足下列条件:*

1) $x = (*, \alpha)\cdots$ 为 2 阶元;

2) 若记 $K = H_\alpha$, 则 x 正规化 K, 即 $K^x = K$.

3) $y \notin K$, 且有 $h_1, h_2 \in H$, 使 $xyx = h_1 x h_2$. 则 $G = \langle x, H\rangle$ 为 H 的一个传递扩张. 反过来，若 H 有传递扩张 G, 则存在满足条件 1), 2), 3) 的 x 和 y, 且 $G = \langle x, H\rangle$.

证 首先设满足 1), 2), 3) 的 x, y 存在，定义集合

$$G = H \cup HxH,$$

我们证明 G 对乘法封闭. 设 $g_1, g_2 \in G$. 若 g_1, g_2 中有一个在 H 内, 则 $g_1g_2 \in G$. 今设 g_1, g_2 都在 HxH 内. 于是有 $a, b, c, d \in H$, 使 $g_1 = axb$, $g_2 = cxd$. 因而 $g_1g_2 = ax(bc)xd$, $bc \in H$. 但 H 在 Ω 上 2 重传递, 因此 $H = K \cup KyK$. 故 $bc \in K$ 或 $bc \in KyK$. 若 $bc \in K$, 由于条件 2) 成立, $xbcx \in K \leq H$, 故 $g_1g_2 \in H$. 若 $bc \in KyK$. 则有 $k_1, k_2 \in K$, 使 $bc = k_1yk_2$. 于是 $g_1g_2 = axk_1yk_2xd = ak_1^x \cdot xyxk_2^x d$. 由条件 3), $xyx = h_1xh_2$, $h_1, h_2 \in H$, 而由条件 2), $k_1^x, k_2^x \in K \subseteq H$. 于是 $g_1g_2 = (ak_1^x h_1)x(h_2k_2^x d) \in HxH$. 故 G 对乘法封闭, 因而 G 为一个群. 由于 H 以 $*$ 为不动点, 而 $*$ 在 HxH 中每个元素下的像都在 Ω 内. 所以 $G_* = H$, $G = \langle x, H\rangle$ 是显然的.

反过来, 若 G 为 H 的传递扩张, G 就在 Ω^* 上 3 重传递. 因而 G 中有一个 2 阶元 x 交换 $*$ 和 α. 又此时 $K = G_{*\alpha}$, 而 $x \in G_{\{*,\alpha\}}$, 所以 x 正规化 K. G 的 3 重传递性使 $G = H \cup HxH$. 因此当 $y \in H$, 但 $\alpha^y \neq \alpha$ 时 $xyx \notin H$, 故 $xyx \in HxH$. 这说明有 $h_1, h_2 \in H$, 使 $yxy = h_1yh_2$. 定理的最后一个结论显然成立. □

利用这个定理我们可以构造出 M_{11} 和 M_{12} 来.

取 $\Omega = \{1, 2, \cdots, 12\}$, 并取

$$\begin{aligned}
u &= (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9),\\
a &= (2\ 4\ 3\ 7)(5\ 6\ 9\ 8),\\
b &= (2\ 5\ 3\ 9)(4\ 8\ 7\ 6),\\
x &= (1\ 10)(4\ 5)(6\ 8)(7\ 9),\\
y &= (10\ 11)(4\ 7)(5\ 8)(6\ 9),\\
z &= (11\ 12)(4\ 9)(5\ 7)(6\ 8).
\end{aligned}$$

定理 7.3 令 $G = \langle u, a, b, x, y, z\rangle$, 则 G 为 Ω 上 5 重传递群, G 的阶为 $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$. 特别 G 为精确 5 重传递群.

证 令 $K = \langle u, a, b\rangle$, $L = \langle u, a, b, x\rangle$, $H = \langle u, a, b, x, y\rangle$.

首先 $v = u^a = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$. 所以 $\langle u, v\rangle$ 为 9 阶初等交换群. 容易验证, $a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1}$, 故 $\langle a, b\rangle$ 为一个四元数群. 它在 $\{2,3,\cdots,9\}$ 上传递. 而 $u^a = v$, $v^a = u^{-1}$, $u^b = uv$,

$v^b = uv^2$. 所以 $\langle u,v\rangle$ 被 $\langle a,b\rangle$ 正规化. 于是 $K = \langle u,v,a,b\rangle$ 为 72 阶群, 且 K 在 $\{1,2,\cdots,9\}$ 上为 2 重传递群. 而 $\langle a,b\rangle$ 为点 1 在 K 中的稳定子群.

我们证明 L 为 K 的传递扩张. 首先 x 为 2 阶元, 它交换 "1" 和 "10". 因 $a^x = b$, $b^x = a$, 故 x 正规化 $\langle a,b\rangle$. u 在 K 内但 $1^u \neq 1$. 且 $xux = ua^2xu$, 其中 $ua^2, u \in K$. 这说明此处的 K, x, u 满足定理 7.2 中关于 H, x, y 的条件 1), 2), 3). 所以 $L = \langle x,K\rangle$ 为 K 的传递扩张. L 为 $\{1,2,\cdots,10\}$ 上的 3 重传递群, $|L| = 10\cdot 9\cdot 8$.

同样办法可以证明 H 为 L 的传递扩张, 因而 H 为 $\{1,2,\cdots,11\}$ 上 4 重传递群, 且 $|H| = 11\cdot 10\cdot 9\cdot 8$, 而 G 为 H 的传递扩张, 为 Ω 上 5 重传递群, $|G| = 12\cdot 11\cdot 10\cdot 9\cdot 8$. 请读者自己补上这些证明.

由 G 的 5 重传递性和 G 的阶可以看出, G 为精确 5 重传递群. □

上述定理中的 H, G 分别记作 M_{11}, M_{12}.

定理 7.4 *M_{11} 和 M_{12} 都是单群.*

证 仍使用定理 7.3 中符号, 于是 $H = M_{11}$, $G = M_{12}$.

先证 H 为单群. 设 $1 \neq N$ 为 H 的正规子群, 由于 H 为 $\{1,2,\cdots,11\}$ 上的本原群, 故 N 在 $\{1,2,\cdots,11\}$ 上传递. 因此 $11 \mid |N|$. 于是 H 有一个 Sylow 11-子群在 N 内, 因而 H 的所有 Sylow 11-子群都在 N 内. 设 H 中有 n_{11} 个 Sylow 11-子群. 则 $n_{11} \equiv 1 \pmod{11}$, 另一方面, 设 P 为 H 的一个 Sylow 11-子群, 那么 $C_H(P) = P$, 因而 $N_H(P)/P$ 同构于 $\mathrm{Aut}(P)$ 的一个子群, 故 $|N_H(P)| \leq 11\cdot 10$. 因而 $n_{11} \geq 9\cdot 8$. 这推出 $n_{11} = 144$. 因此 $|N| \equiv 0 \pmod{11\cdot 144}$. $N \neq H$ 时必有 $|N| = 11\cdot 144$. 此时 P 在 N 内的正规化子就是 P 本身. 依 Burnside 定理 (上册, 第 II 章定理 5.4), P 在 N 内有正规补群, 后者作为 N 的特征子群应为 H 的正规子群, 但其阶与 11 互素, 这与 H 的正规子群在 $\{1,2,\cdots,11\}$ 上传递的事实矛盾. 故 $N = H$. H 为单群.

G 在 Ω 上为 5 重传递群. 设 $1 \neq N$ 为 G 的正规子群. 若 N 在 Ω 上正则, 则 $|N| = 12$, 但 N 作为 G 的极小正规子群, 其阶应为素数方幂. 所以 N 在 Ω 上非正则. 取 $\alpha = 12 \in \Omega$, 则 $1 \neq N_\alpha \lhd G_\alpha = H$, 由 H 的单性知 $N_\alpha = H$, 进而 $N = G$. 这就证明了 G 的单性. □

本世纪 30 年代 Witt 发现 Mathieu 群与一种称为 t-设计的组合结构有紧密的联系. 我们来考察 M_{12} 与 t-设计的联系.

定义 7.5 设 v, k, λ, t 为正整数, 且 $v > k > t \geq 2$. 设 P 为一个 v 元集合, 其中元素称为点, $\mathcal{B}$ 是由 P 的若干特定的 k 元子集 (它们称为区组) 所组成的集合, 并且对 P 的任何一个 t 元子集 Δ, 恰好有 $\mathcal{B}$ 中 λ 个区组包含 Δ, 则称体系 $\mathcal{D} = (P, \mathcal{B})$ 为一个 t-(v, k, λ) 设计, 简称 t-设计.

例 7.6 设 $\Omega = \{1,2,3,4,5,6,7\}$, $\mathcal{B}$ 由下面 7 个区组组成

$$\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}$$

$$\{5,6,1\}, \{6,7,2\}, \{7,1,3\}.$$

则不难验证 $(\Omega, \mathcal{B})$ 为一个 2-(7,3,1) 设计.

在 t-设计的定义中出现了参数 v, k, λ, t. 但它还有一些重要参数, 我们首先考察一个 t-(v,k,λ) 设计中区组的总数 b. 计算形如 (Σ, B) 的 "对" 的总数, 其中 Σ 表示一个 t 元集, B 表示区组, 且满足 $\Sigma \subseteq B$. P 的 t 元子集有 $\binom{v}{t}$ 个, 每个 t 元子集 Σ 包含在 λ 个区组内. 所以这样的 "对" 有 $\lambda\binom{v}{t}$ 个. 另一方面我们总共有 b 个区组, 每个区组中包含 $\binom{k}{t}$ 个 t 元子集, 所以这样的对有 $b\binom{k}{t}$ 个. 于是我们得到

$$\lambda\binom{v}{t} = b\binom{k}{t}.$$

这说明

$$b = \lambda\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}, \tag{7.1}$$

即区组总数 b 可由参数 v, k, λ, t 给出.

再考察在 t-设计 $\mathcal{D}=(P,\mathcal{B})$ 中，一个给定的 $t-1$ 元子集 Δ 出现在多少区组中. 计算下列形状的对的个数: (Σ, B), 其中 $\Sigma \supseteq \Delta$ 为 t 元集， B 为包含 Σ 的区组. 设有 λ_{t-1} 个 B 包含 Δ. 由于 Σ 的取法有 $v-t+1$ 个. 每个 Σ 包含在 λ 个区组内，这样的对有 $\lambda(v-t+1)$ 个. 而一旦 $B \supseteq \Delta$, 则 B 中有 $k-t+1$ 个包含 Δ 的 t 元子集. 这样一来，又有等式

$$\lambda(v-t+1)=\lambda_{t-1}(k-t+1).$$

于是

$$\lambda_{t-1}=\lambda\frac{v-t+1}{k-t+1}. \tag{7.2}$$

这说明在 $\mathcal{D}$ 中，每个 $t-1$ 元子集恰好包含在 λ_{t-1} 个区组内. 根据定义 7.5, $\mathcal{D}$ 同时又是一个 $(t-1)$-(v,k,λ_{t-1}) 设计. 其中 λ_{t-1} 由 (7.2) 式给出. 继续上边的过程，我们可知一个 t-(v,k,λ) 设计总是一个 s-(v,k,λ_s) 设计，其中 $2 \le s \le t$, 而 λ_s 由

$$\lambda_s=\lambda\frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)} \tag{7.3}$$

给出. 特别对 $t \geq 2$, 每个 t-设计都是一个 2-设计. 我们通常用 r 表示 λ_1, 它表示 P 中每个点恰出现在 r 个区组内. 显然 $r=\frac{bk}{v}$.

为研究 t-设计，我们常使用矩阵方法. 设 $\mathcal{D}$ 为一个 t-(v,k,λ) 设计，其中有区组 b 个. 设 $P=\{p_1,\cdots,p_v\}$, 区组为 $B_1, B_2, \cdots, B_b$. 由 $\mathcal{D}$ 我们定义一个 $v \times b$ 矩阵 $A=(a_{ij})$, 其中

$$a_{ij}=\begin{cases}1 & 若 p_i \in B_j,\\ 0 & 若 p_i \notin B_j.\end{cases} \tag{7.4}$$

A 称为 $\mathcal{D}$ 的关联矩阵, 关联矩阵 A 为 $(0,1)$ 矩阵. 易知 $\mathcal{D}$ 和 A 相互唯一确定. A 的“行和”表示一个点 p 落在多少个区组内，所以为 r. A 的“列和”表示一个区组内有多少点，故为 k.

定理 7.7 *在 t-(v,k,λ) 设计 $\mathcal{D}$ 中，若 $t \geq 2$, 则 $b \geq v$.*

证 由于每个 t-设计, $t \geq 2$, 总是一个 2-设计. 我们不妨设 $t=2$, 并把相应的 λ_2 还记作 λ. 于是我们有

$$AA^t = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \cdot & \cdot & \cdots & \cdot \\ \lambda & \lambda & \cdots & r \end{pmatrix} \tag{7.5}$$

这里 A^t 表示 A 的转置. 实际上, AA^t 中 (i,j) 位置的元素就是和 $\sum_{k=1}^{b} a_{ik}a_{jk}$. 当 $i=j$ 时这表示 A 的第 i 行中有多少个 1. 在 $i \neq j$ 时表示 A 的第 i 行和第 j 行中有多少个位置同时为 1. (7.5) 的右端的矩阵的行列式为

$$\det(AA^t) = (r + (v-1)\lambda)(r-\lambda)^{v-1}.$$

由于 $r > \lambda$(请读者证明), 所以 AA^t 的秩为 v, 进而 A 的秩为 v, 这说明 $b \geq v$.

我们再举两类设计的例子

例 7.8 设 $\mathbf{F} = GF(q)$ 为有限域, $n \geq 2$, V 为 $\mathbf{F}$ 上的 $n+1$ 维向量空间. 在定义 3.12 中我们已定义了射影空间 $PG(n,\mathbf{F})$, 在那里 V 的一维子空间叫做 $PG(n,\mathbf{F})$ 中的点. $PG(n,\mathbf{F})$ 中点的全体组成集合 P. 把 V 中 2 维子空间 (看成一维子空间的集合) 称为 $PG(n,\mathbf{F})$ 中的线. 把线叫做区组. 由于 V 任何两个不同一维空间恰生成 V 中一个 2 维子空间, 我们就得到了一个 2-$(v,k,1)$ 设计, 这里 $v = q^{n+1} - 1/q - 1$, $k = q+1$. 当 $n=2$ 时, 称这个设计为 **有限射影平面**. 此时 $v = b = q^2+q+1$. 一个 2-设计, 若 $v=b$ 则称为 **对称区组设计**. 不难看出例 7.6 是有限射影平面 $PG(2,2)$, 这里不写成 $PG(2,\mathbf{F})$ 而写成 $PG(2,2)$, 表示 $|\mathbf{F}| = 2$.

例 7.9 设 $\mathbf{F} = GF(q)$, $n \geq 2$ 为整数. V 为 $\mathbf{F}$ 上 n 维向量空间, 把 V 中向量称为 **点**, 把 V 的 1 维子空间在 V(看成加法群) 内的陪集 (称为直线) 看成区组, 我们又得到一个 2-$(v,k,1)$ 设计

$\mathcal{D}$, 其中 $v=q^n$, $k=q$. 当 $n=2$ 时我们称 $\mathcal{D}$ 为**仿射平面**, 此时 $v=q^2$, $k=q$, $b=q^2+q$.

设 $\mathcal{D}$ 为一个 t-(v,k,λ) 设计, $t\geq 2$. p 为 $\mathcal{D}$ 中一点. 我们可构造一个新的设计 $\mathcal{D}_p$: 点集为 $P-\{p\}$, 区组形如 $B-\{p\}$, 其中 B 为 $\mathcal{D}$ 的包含点 p 的区组. 容易验证 $\mathcal{D}_p$ 为一个 $(t-1)$-$(v-1,k-1,\lambda)$ 设计. $\mathcal{D}_p$ 称为 $\mathcal{D}$ **在点 p 处的收缩**.

设 $\mathcal{D}=(P,\mathcal{B})$ 为一个 t-(v,k,λ) 设计. g 为 P 的一个置换, 如果对 $\mathcal{D}$ 中任一区组 B, $B^g=\{p^g \mid p\in B\}$ 仍是 $\mathcal{D}$ 的区组. 则 g 称为 $\mathcal{D}$ 的**自同构**. $\mathcal{D}$ 的全体自同构组成一个群, 称为 $\mathcal{D}$ 的**自同构群**, 记作 $\mathrm{Aut}(\mathcal{D})$.

设计是一类重要的组合结构. 对它们的研究成为组合数学的一个重要分支. 它与群论有密切的联系. 现在我们回到 M_{12} 上来.

仍设 $G=M_{12}$ 作用于 $\Omega=\{1,2,\cdots,12\}$ 上, 而且由 u, a, b, x, y, z 生成. 记 $\Delta=\{1,2,3,10,11,12\}$. 用 $G_{\{\Delta\}}$ 表示 Δ 在 G 内的集型稳定子群. 显然 u, $x,y,z\in G_{\{\Delta\}}$, 并且 $u^\Delta=(1,2,3)$, $x^\Delta=(1,10)$, $y^\Delta=(10,11)$, $z^\Delta=(11,12)$. 由此知 $G_{\{\Delta\}}^\Delta\cong S_6$. 另一方面, 因为 G 为精确 5 重传递群, 所以 $G_{(\Delta)}=1$. 于是 $G_{\{\Delta\}}=\langle u,x,y,z\rangle$ 忠实地作用于 Δ 上.

定理 7.10 *设 G 为 Ω 上的 t 重传递群. $\Delta\subseteq\Omega$, $|\Delta|=k>t$. 若 $G_{\{\Delta\}}$ 在 Δ 上为 t 重传递群, 而 Δ 中有 t 个元素 $\alpha_1,\cdots,\alpha_t$, 使 $G_{\alpha_1,\cdots,\alpha_t}\leq G_{\{\Delta\}}$. 那么令 $\mathcal{B}=\{\Delta^g \mid g\in G\}$ 为区组集合, 则 $\mathcal{D}=(\Omega,\mathcal{B})$ 为一个 t-$(v,k,1)$ 设计. 其中 $v=|\Omega|$. 此时 G 的每个元素都是 $\mathcal{D}$ 的自同构.*

证 只需证对 Ω 中任意 t 个点 $\beta_1,\beta_2,\cdots,\beta_t$, 有且有唯一的 Δ^g 包含它们. 因为 G 在 Ω 上 t 重传递, 所以有 $g\in G$, 使 $\beta_1=\alpha_1^g,\cdots,\beta_t=\alpha_t^g$. 此时 $\beta_1,\cdots,\beta_t\in\Delta^g$. 若有 $h\in G$ 使 Δ^h 也包含 $\beta_1,\cdots,\beta_t$. 则在 Δ 中有 $\gamma_1,\gamma_2,\cdots,\gamma_t$ 使 $\gamma_1^h=\beta_1,\cdots,\gamma_t^h=\beta_t$. 而 $G_{\{\Delta\}}$ 在 Δ 是 t 重传递的, 所以有 $k_1\in G_{\{\Delta\}}$, 使 $\alpha_1^{k_1}=\gamma_1,\cdots,\alpha_t^{k_1}=\gamma_t$. 这样一来对一切 i, $\alpha_i^{k_1h}=\beta_i$. 故 $k_1hg^{-1}=k_2\in G_{\alpha_1\cdots\alpha_t}\leq$

$G_{\{\Delta\}}$. 令 $k_1^{-1}k_2 = k$, 则 $h = kg$ 而 $k \in G_{\{\Delta\}}$. 于是 $\Delta^h = \Delta^{kg} = \Delta^g$, 这说明只有一个 Δ^g 包含 $\beta_1, \cdots, \beta_t$. $(\Omega, \mathcal{B})$ 为 t-$(v,k,1)$ 设计. 最后一个结论是显然的. □

应用这个定理我们得到

定理 7.11 *存在一个 5-(12,6,1) 设计 $\mathcal{D}$, 使 $G = M_{12}$ 的每个元素都是 $\mathcal{D}$ 的自同构.*

证 令 $\Omega = \{1,2,\cdots,12\}$, $\Delta = \{1,2,3,10,11,12\}$. 由于 $G_{\{\Delta\}}^{\Delta}$ 在 Δ 上为 5 重传递的. 而 $G_{1,2,3,10,11} = 1 \leq G_{\{\Delta\}}$. 又 G 为 Ω 上 5 重传递群. 故由 7.10 知 $\mathcal{D} = (\Omega, \mathcal{B})$, 其中

$$\mathcal{B} = \{\Delta^g \bigm| g \in G\},$$

是一个 5-(12,6,1) 设计, 并且 $G = M_{12}$ 中每个元素都是 $\mathcal{D}$ 的自同构. □

现在我们已得到了一个 5-(12,6,1) 设计 $\mathcal{D}$. 我们来研究 $\mathcal{D}$ 内的组合问题. 首先, 由 (7.1) 和 (7.3) 知

$$b = 132, \lambda_1 = 66, \lambda_2 = 30, \lambda_3 = 12, \lambda_4 = 4.$$

设 Δ 为一个区组, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 为 Δ 中的点. 由 $\lambda_4 = 4$, 知有三个不同于 Δ 的区组与 Δ 交于 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, 写 $\mu_4 = 3$, 知这个数与 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 的取法无关. 再计算与 Δ 恰好交于 $\alpha_1, \alpha_2, \alpha_3$ 的区组数. B 中包含 $\alpha_1, \alpha_2, \alpha_3$ 的 4 元集有 3 个. 故在过 $\alpha_1, \alpha_2, \alpha_3$ 的 12 个区组内, 有 $3\mu_4 = 9$ 个与 Δ 交于 4 个点, 除去这 9 个区组和 Δ 本身, 剩下的 2 个区组与 B 交于 $\alpha_1, \alpha_2, \alpha_3$. 写 $\mu_3 = 2$, μ_3 也与 $\alpha_1, \alpha_2, \alpha_3$ 的取法无关. 类似地可以计算 μ_2, μ_1. 于是有

$$\mu_4 = 3, \mu_3 = 2, \mu_2 = 3, \mu_1 = 0.$$

这样一来, 由于 $132 - (3 \cdot \binom{6}{4} + 2 \cdot \binom{6}{3} + 3 \cdot \binom{6}{2} + 1) = 1$, 说明恰有一个区组与 Δ 的交为空集, 这个区组就是 Δ 在 Ω 中的余集 $\overline{\Delta}$. 利用这一事实, 定理 7.11 可加强为:

定理 7.12 *群 $G = M_{12}$ 为上边所构造的 5-(12,6,1) 设计 $\mathcal{D}$ 的自同构群.*

证 记 $A = \mathrm{Aut}(\mathcal{D})$. 我们已看到 $G \le A$. 今设 $G < A$. 由于 G 在全体区组上传递, A 也在全体区组上传递. 于是对一个给定的区组, 例如 Δ, $G_{\{\Delta\}} < A_{\{\Delta\}}$. 由于 $G_{\{\Delta\}}^{\Delta} \cong S_6$, 所以 $A_{(\Delta)} \ne 1$. 但 $A_{(\Delta)} \lhd A_{\{\Delta\}}$, 于是 $G_{\{\Delta\}}$ 正规化 $A_{(\Delta)}$. 特别 $G_{\{\Delta\}}^{\overline{\Delta}}$ 正规化 $A_{(\Delta)}^{\overline{\Delta}} \ne 1$. 因为 $\overline{\Delta}$ 也是区组, 故 $G_{\{\Delta\}}^{\overline{\Delta}} \cong S_6$. 因而 $A_{(\Delta)}^{\overline{\Delta}}$ 包含 $\overline{\Delta}$ 上交错群. 这说明 $A_{(\Delta)}$ 中包含一个 3 轮换. 这使得 A 包含 Ω 上交错群. 这与 A 为 $\mathcal{D}$ 的自同构群的假设矛盾. 定理成立. □

在 $\Omega = \{1, 2, \cdots, 12\}$ 中取一点 p, 比如 $p = 12$. 那么 $\mathcal{D}$ 在 p 处的收缩为一个 4-(11,5,1) 设计 $\mathcal{D}_p$. 显然 $H = M_{11}$ 包含在 $\mathrm{Aut}(\mathcal{D}_p)$ 内. 我们同样可证明 $M_{11} = \mathrm{Aut}(\mathcal{D}_p)$. 进而我们还得到一个 3-(10,4,1) 设计和一个 2-(9,3,1) 设计. 注意这最后一个 2-设计是定义于 $GF(3)$ 上的仿射平面.

本节的讨论未证明 M_{12}, M_{11} 的唯一性, 即我们没有回答是否有 12 级精确 5 重传递群与 G 不是置换同构的问题. 这个问题可通过本章后面有关习题来回答.

关于 Mathieu 群 M_{24}, M_{23}, M_{22} 可以类似地处理. 同样也可得到相应的 5-(24,8,1) 设计, 4-(23,7,1) 设计和 3-(22,6,1) 设计. 这些我们不再讨论.

§8. 素数级本原群

在本节中, 我们用表示论的方法来处理置换群的问题. 除了表示, 特征标, 分裂域等概念和一些基本理论外, 我们还要用到某些事实和概念.

定理 8.1 *设 G 为有限群, ρ 为复数域 $\mathbb{C}$ 中一个 $|G|$ 次本原单位根, 则 $\mathbb{Q}(\rho)$ 是 G 的分裂域.*

这个定理是 Brauer 首先证明的. 此处我们不加证明地使用. 今设 $\mathbf{D}$ 为 G 在某个域 $\mathbf{F}(\subset \mathbb{C})$ 上的表示, 其中 $\mathbf{F}$ 为 $\mathbb{Q}$ 的有限扩

张. 必要时通过扩张, 我们还可以假设 $\mathbf{F}$ 在 $\mathbb{Q}$ 上是 Galois 的, 其 Galois 群由 $\mathbf{F}$ 的自同构组成.

定义 8.2 设 $\mathbf{D}$ 为群 G 在域 $\mathbf{F}$ 上的 (矩阵) 表示. α 为 $\mathbf{F}$ 的一个自同构. 设 $g \in G$, $\mathbf{D}(g)$ 为 g 在 $\mathbf{D}$ 下的表示矩阵. 把 $\mathbf{D}(g)$ 中每个元素 a_{ij} 用它在 α 下的共轭 a_{ij}^{α} 代替, 得到一个新的矩阵 $\mathbf{D}^{\alpha}(g)$. 则 $\mathbf{D}^{\alpha}: g \mapsto \mathbf{D}^{\alpha}(g), \forall g \in g$, 是 G 在 $\mathbf{F}$ 上的一个表示. 若 $\mathbf{D}$ 与 $\mathbf{D}^{\alpha}$ 不等价, 则称 $\mathbf{D}$ 与 $\mathbf{D}^{\alpha}$ 是代数共轭的表示. 用 χ^{α} 记 $\mathbf{D}^{\alpha}$ 的特征标, 则 $\chi^{\alpha}(g) = (\chi(g))^{\alpha}, \forall g \in G$. χ 与 χ^{α} 也称为代数共轭的.

定义中关于 $\mathbf{D}^{\alpha}$ 为表示, $\chi^{\alpha}(g) = (\chi(g))^{\alpha}$ 这两个结论是明显的. 同样明显的, $\mathbf{D}$ 不可约时 $\mathbf{D}^{\alpha}$ 也不可约, χ 不可约时 χ^{α} 也不可约. 我们还知道, 若 $\mathbf{F}$ 就是定理 8.1 中的 $\mathbb{Q}(\rho)$, 那么 $\mathbf{F}$ 的自同构都可由 $\rho \mapsto \rho^k$ 确定, 这里 k 为整数且 $(k, |G|) = 1$.

下面我们建立置换群表示论的基本事实.

设 G 为 $\{1, 2, \cdots, n\}$ 上的置换群. 取复数域 $\mathbb{C}$ 上的 n 维向量空间 V, 并取定一组基 $v_1, v_2, \cdots, v_n$. 设 $g \in G$, 把 g 对应一个线性变换 $\hat{g}$:, 若 $i^t = j$, 则 $v_i^{\hat{g}} = v_j$. 于是 $g \mapsto \hat{g}$ 就定义了 G 在 V 上的表示. $\hat{g}$ 在上述基下的矩阵为 $(g_{ij})_{n \times n}$, 其中 $g_{ij} = 0$ 或 1, 而 $g_{ij} = 1$ 当且仅当 $i^g = j$. 这个表示在第 IV 章例 1.7 中称为 G 的置换表示. 它的特征标记作 π, 明显地 $\pi(g)$ 正好是置换 g 在 Ω 上的不动点的个数. (见第 IV 章例 5.3).

我们仍使用下面的记号: 若 χ, ψ 为 G 的特征标, $\langle \chi, \psi \rangle = \frac{1}{|G|} \sum\limits_{g \in G} \chi(g) \overline{\psi(g)}$.

定理 8.3 若 G 在 Ω 上有 t 个轨道, 则 $\langle 1_G, \pi \rangle = t$, 其中 1_G 是 G 的主特征标.

证 考虑集合

$$\Theta = \{(\alpha, g) \mid \alpha \in \Omega, g \in G, \text{ 且} \alpha^g = \alpha\}$$

明显地，$|\Theta| = \sum_{g\in G} \pi(g)$. 现设 G 在 Ω 上的 t 个轨道为 $\Omega_1, \Omega_2, \cdots, \Omega_t$. 其中 $|\Omega_i| = n_i$. 设 $\alpha \in \Omega_i$, 则 $(\alpha, g) \in \Theta$ 当且仅当 $g \in G_\alpha$. 所以 α 给出 $|G|/n_i$ 个对 $(\alpha, g) \in \Theta$. 这样一来 $|\Theta| = \sum_{i=1}^{t} \sum_{\alpha\in\Omega_i} |G|/n_i = t|G|$. 于是 $\langle 1_G, \pi\rangle = \frac{1}{|G|} \sum_{g\in G} \pi(g) = t$. 证完. □

推论 8.4 *若 G 在 Ω 上传递，则主特征标在 π 中的重数为 1.*

在 §4 中我们看到，当在 Ω 上传递时， G 可看成 $\Omega\times\Omega$ 上的置换群. 此时 G 在 $\Omega\times\Omega$ 上的轨道数等于 G_α $(\alpha\in\Omega)$ 在 Ω 上的轨道数，等于 G 的秩 r. 另一方面， G 作为 $\Omega\times\Omega$ 上的置换群时，其相应的置换表示的特征标为 π^2. 由定理 8.3 我们得到：

定理 8.5 *设 G 为 Ω 上置换群，它相应的特征标为 π. 若 G 的秩为 r, 则 $\langle\pi, \pi\rangle = r$.*

把 π 分解成复数域上不可约特征标之和. 得

$$\pi = a_0\chi_0 + a_1\chi_1 + \cdots + a_s\chi_s,$$

其中 $\chi_0 = 1_G$, $\chi_0, \chi_1, \cdots, \chi_s$ 各不相同， $a_0, a_1, \cdots, a_s$ 为其各自在 π 内的重数. 由定理 8.5, 知 $a_0^2 + a_1^2 + \cdots + a_s^2 = r$. 由推论 8.4, 知当 G 传递时， $a_0 = 1$. 所以又推出

推论 8.6 *G 在 Ω 上为 2 重传递群当且仅当 G 的置换特征标 π 为主特征标与一个不可约特征标之和.*

现在我们来证明本节的主要定理.

定理 8.7 *素数级本原群要么是 2 重传递群，要么是可解群.*

证 设 $|\Omega| = p$ 为素数， G 为 Ω 上本原群. 假设 G 在 Ω 上不是 2 重传递的，我们来证明 G 为可解群.

G 的 Sylow p-子群为 p 阶循环群，即 $P = \langle x\rangle$, x 为 p 长轮换. 由于 $C_G(P) = P$, 故 $N_G(P)/P$ 同构于 $\mathrm{Aut}(P) = Z_{p-1}$ 的子群，于是 $|N_G(P)|$ 为 $p(p-1)$ 的因子.

因 G 传递但非 2-传递，所以若仍用 π 表示 G 的置换特征标时，$\langle\pi, 1_G\rangle = 1$. $\langle\pi,\pi\rangle > 2$. 于是 π 有分解式

$$\pi = \chi_0 + \alpha_1\chi_1 + \cdots + \alpha_s\chi_s$$

其中 χ_0 为 G 的主特征标，$\chi_0, \chi_1, \cdots, \chi_s$ 各不相同，a_i 为 χ_i 在 π 内的重数.

我们证明下列各点：

1) $a_1 = a_2 = \cdots = a_s = 1$.

由于 P 交换，P 有 p 个不可约特征标 $\varphi_0, \varphi_1, \cdots, \varphi_{p-1}$. 把 π 限制到 P 上，它正好是 P 的正则表示. 所以 $\pi|_P = \sum_{i=0}^{p-1} \varphi_i$. 由于每个 φ_i 在 $\pi|_P$ 内重数为 1, 所以知 π 的每个成分 χ_j 在 π 中重数为 1, 由此

$$\pi = \chi_0 + \chi_1 + \cdots + \chi_s.$$

于是 $\langle\pi,\pi\rangle = 1 + s \geq 2$. 此时 P 的每个不可约特征标 φ_j 恰出现在某个特定的 $\chi_i|_P$ 内.

2) $\chi_1, \cdots, \chi_s$ 是相互代数共轭的，特别它们的次数相等，并且若 $1 \neq y \in G$, 且 y 的阶与 p 互素，那么 y 在各 $\chi_i, 1 \leq i \leq s$, 中取值相同.

设 $\rho \in \mathbb{C}$ 为 $|G|$ 次本原单位根. 令 $\omega = \rho^p$, $\varepsilon = \rho^{|G|/p}$, 则 ω, ε 分别为 $|G|/p$ 次和 p 次本原单位根. 此时可视 $\chi_i, 1 \leq i \leq s$, 为 G 在 $\mathbf{F} = \mathbb{Q}(\rho)$ 上的特征标. 令 $L = \mathbb{Q}(\omega)$, 则 $\mathbf{F} = L(\varepsilon)$. 我们把 P 的不可约特征标如此排列，使 $\varphi_j(x) = \varepsilon^j$. 今设 φ_1 为 $\chi_1|P$ 的成分，而 $\varphi_j, 1 < j \leq p-1$, 为 χ_i 的成分. 取一个整数 u, 使 $u \equiv j (\mathrm{mod}\ p)$ 而 $u \equiv 1 (\mathrm{mod}\ |G|/p)$. 此时 $(u, |G|) = 1$. 于是有 $\mathbf{F}$ 在 $\mathbb{Q}$ 上的自同构 α, 使 $\rho^\alpha = \rho^u$. 此时 $\omega^\alpha = \omega$, 故 α 把 L 中每个元素不变. 于是 $\varphi_1^\alpha = \varphi_j$, 而 $(\chi_1^\alpha)|_P = (\chi_1|_P)^\alpha$ 包含 φ_j 为不可约成分. 但

$$1 = \langle\chi_1, \pi\rangle^\alpha = \langle\chi_1^\alpha, \pi\rangle.$$

所以 χ_1^α 为 $\chi_1, \chi_2, \cdots, \chi_s$ 中的一个，因此 χ_1^α 只能是包含 φ_j 的成分 χ_i. 这说明每个 χ_i 都与 χ_1 是代数共轭的. 若 y 的阶与 p 互

素，则 $\chi_1(y)$ 为 $|G|/p$ 次单位根之和，故 $\chi_1(y) \in L$, 而 α 不变 L 中元素，所以 $\chi_i(y) = \chi_1^\alpha(y) = \chi_1(y)^\alpha = \chi_1(y)$.

3) 若 $1 \neq y \in G$ 的阶 $o(y)$ 与 p 互素，则 $\chi_1(y)$ 为非负整数，并且 $\chi_1(y) \leq t$, 其中 $st = p-1$.

我们有 $\pi(y) = 1 + \sum\limits_{i=1}^{s} \chi_i(y) = 1 + s\chi_1(y)$. 由于 $\pi(y) \geq 0$ 为整数，所以 $\chi_1(y)$ 为有理数. 但 $\chi_1(y)$ 又是代数整数，故 $\chi_1(y)$ 为有理整数. 而 $0 \leq \pi(y) \leq p$, 所以 $\chi_1(y)$ 为非负的，且 $\chi_1(y) \leq p-1/s = t$.

由于 $C_G(P) = P$, 所以 G 中元素的阶要么为 p, 要么与 p 互素. 设 G 中有 N_i 个阶与 p 互素的元素 y 满足 $\chi_1(y) = i$. 并设 G 有 l 个 Sylow p-子群.

4) $\sum\limits_{i=1}^{t} iN_i = lt$, $\sum\limits_{i=1}^{t} i^2 N_i = lt^2$.

计算 $\langle 1, \chi_1 \rangle$ 得

$$0 = |G|\langle 1, \chi_1 \rangle = \sum_{g \in g} \chi_1(g) = \sum_{o(g) \neq p} \chi_1(g) + \sum_{o(g)=p} \chi_1(g)$$

$$= \sum_{i=1}^{t} iN_i + l\sum_{j=0}^{p-1} \chi_1(x^j) - l\chi_1(e) = \sum_{i=1}^{t} iN_i - lt.$$

其中用 e 表示 G 的单位元. 这得到第一个等式

再计算 $\langle \chi_1, \chi_2 \rangle$, 得

$$\begin{aligned} 0 &= |G|\langle \chi_1, \chi_2 \rangle = \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} \\ &= \sum_{o(g) \neq p} \chi_1^2(g) + \sum_{o(g)=p} \chi_1(g)\overline{\chi_2(g)} \\ &= \sum_{i=1}^{t} i^2 N_i + l\sum_{j=0}^{p-1} \chi_1(x^j)\overline{\chi_2(x^j)} - lt^2 \\ &= \sum_{i=1}^{t} i^2 N_i - lt^2. \end{aligned}$$

最后一个等号因为 P 的每个不可约特征标不能同时出现于 $\chi_1|_P$ 和 $\chi_2|_P$ 中. 第二个等式成立.

5) 定理成立.

把 4) 中的第一个等式乘以 t, 再减去第二个等式，得

$$t\sum_{i=1}^{t} iN_i - \sum_{i=1}^{t} i^2 N_i = \sum_{i=1}^{t} i(t-i)N_i = 0$$

这说明 $N_1 = N_2 = \cdots = N_{t-1} = 0$. 所以若 G 中元素 y 的阶与 p 互素，则 $\pi(y) = 1$ 或 $y = 1$(因而 $\pi(y) = p$). 因此 G 为一个 Frobenius 群． G 的 Sylow p-子群 $P \lhd G$, 且 G/P 为循环群，故 G 为可解群.

至此定理证完 □

我们来看一些例子.

例 8.8 设 $\mathbf{F} = GF(q)$. $\mathbf{F}$ 上的一次仿射变换群 $AGL(1,\mathbf{F})$ 由形如

$$\sigma_{a,b} : x \mapsto ax + b,\ a, b \in \mathbf{F}, a \neq 0$$

的变换组成． $AGL(1,\mathbf{F})$ 也写作 $AGL(1,q)$. 它 2 重传递地作用于 $\mathbf{F}$ 上．它是可解群．其中

$$\sigma_{1,b} : x \mapsto x + b,\ b \in \mathbf{F}$$

组成 $AGL(1,\mathbf{F})$ 的正规子群称为 *平移群*. 于是在 $q = p$ 为素数时， $AGL(1,p)$ 的所有包含平移群的子群，给出可解的素数级本原群．反过来，所有可解的 p 级本原群都可视为 $AGL(1,p)$ 的子群.

我们还有一些素数级本原群．如 A_p 和 S_p, p 为素数； M_{11} 和 M_{23}; $PSL(n,q)$ 作用于射影空间 $PG(n-1,q)$ 的点集上，若点的总数 $q^n - 1/q - 1$ 为素数时，也给出素数级本原群的例子.

例 8.9 $PSL(2,7) \cong PSL(3,2) = SL(3,2)$ 是第二个阶最小的单群，把 $SL(3,2)$ 看成二元域上 3 维空间的线性变换群，它 2-传递地作用于非零向量上．于是 $PSL(2,7)$ 可以表示成级数为 7 的本原群.

例 8.10 取 $G = PSL(2,11)$, $G \cong SL(2,11)/Z(SL(2,11))$. 令 $Z = Z(SL(2,11))$. 我们证明 G 可以表示成一个 11 级本原群.

用 $0, 1, \cdots, 10$ 表示 $GF(11)$ 中的元素, 加法和乘法在模 11 的意义下进行. 此时 $SL(2,11)$ 的元素为 $GF(11)$ 上的可逆 2×2 方阵, G 中元素可写成 aZ, 其中 $a \in SL(2,11)$.

取

$$a = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}, b = \begin{pmatrix} 8 & 1 \\ 1 & 3 \end{pmatrix},$$

那么

$$a^5 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, b^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$(ab)^3 = \begin{pmatrix} 5 & 2 \\ 6 & 7 \end{pmatrix}^3 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}.$$

这样一来 $(aZ)^5 = (bZ)^2 = (aZ \cdot bZ)^3$. 由上册第 I 章 §6 的习题 3, 知 $\langle a, b\rangle/Z$ 为 $PSL(2,11)$ 中的 60 阶子群. $|PSL(2,11)| = 660$, 于是 $PSL(2,11)$ 可表示成一个 11 级本原群.

Galois 证明了, 当 $PSL(2,p)$ 为单群时, 只有 $p = 5, 7, 11$ 时可表示成 p 次置换群.

§9. 2 重传递群介绍

本节介绍 2 重传递群的分类. 我们通常把置换群分成三个层次: 传递但非本原群, 本原但非 2 重传递群, 2 重 (以及 2 重以上) 传递群. 置换群现有理论主要是对后两类群加以研究. 对 2 重传递群, 借助有限单群分类定理已经得到了完全分类.

2 重传递群的分类的起点是下面的 Burnside 定理.

定理 9.1 (Burnside) 设 G 是 Ω 上的 2 重传递群, 则要么 G 有一个初等交换的正则正规子群, 要么 G 为几乎单群.

证 设 M 为 G 的一个极小正规子群. 则 M 为相互同构的单群的直积. 由于 G 在 Ω 上为 2 重传递的, M 在 Ω 上正则或为 $\frac{3}{2}$ 重传递群.

若 M 在 Ω 上正则, 由于 G_α 在 $\Omega-\{\alpha\}$ 上传递, M 中任意两个非单位元素 x,y 都在 G_α 下共轭, 因而有相同的阶. 这样一来 M 为初等交换 p-群.

今设 M 在 Ω 上不是正则的. 则 $M=T_1\times\cdots\times T_m$, $T_i\cong T$ 为非交换单群. $m\geq 1$. 此时 M 是 G 的仅有的极小正规子群. 所以 M 就是 G 的基柱. 今设 $m\geq 2$. 取 $\alpha\in\Omega$, 考虑 M_α 的结构. 根据定理 5.8, 要么 $M_\alpha=R_1\times\cdots\times R_m$, 其中 $1\neq R_i$ 为 T_i 的一个真子群且 $R_i\cong R_1$, $\forall i=1,2,\cdots,m$, 要么 M_α 的阶形如 $|T|^s$, 其中 $s\mid m$.

设 M_α 的阶形如 $|T|^s$, $s\mid m$. 设 M_α 在 $\Omega-\{\alpha\}$ 上有一个轨道长为 l. 则因 M_α 在 $\Omega-\{\alpha\}$ 上为 $\frac{1}{2}$ 传递的. 所以 M_α 在 $\Omega-\{\alpha\}$ 的每个轨道长为 l. 这样一来 $l\mid |\Omega|-1$, 而 $|\Omega|=|T|^{m-s}$, 故 $(l,|T|)=1$. 另一方面 M_α 的阶为 $|T|^s$, 所以又应有 $l\mid |T|^s$. 这只有 $l=1$. 因而 M 为正则的, 矛盾.

再设 $M_\alpha=R_1\times\cdots\times R_m$, $m\geq 2$, $R_i<T_i$. 由于 T_1,T_2 为单群, R_1,R_2 为 T_1,T_2 的非单位真子群, 故 $R_i\ntrianglelefteq T_i$. 特别有 $a_1\in T_1$, $a_2\in T_2$ 使 $R_1^{a_1}\neq R_1$, $R_2^{a_2}\neq R_2$. 在 M 中取元素 $g=(a_1,1,\cdots,1)$, $h=(a_1,a_2,1,\cdots,1)$. (此处沿用 §5 中的记号). 则 $M_\alpha^g=R_1^{a_1}\times R_2\times\cdots\times R_m$, $M_\alpha^h=R_1^{a_1}\times R_2^{a_2}\times R_3\times\cdots\times R_m$. 于是 $|M_\alpha:M_\alpha\cap M_\alpha^g|=|R_1:R_1\cap R_1^{a_1}|$, $|M_\alpha:M_\alpha\cap M_\alpha^h|=|R_1:R_1\cap R_1^{a_1}|\cdot|R_2:R_2\cap R_2^{a_2}|$. 但易知这是 $\beta=\alpha^g$ 和 $\gamma=\alpha^h$ 所在的 M_α 的轨道的长度. 因 $|R_2:R_2\cap R_2^{a_2}|>1$, 这与 M 在 Ω 上 $\frac{3}{2}$ 重传递矛盾.

于是当 $M_\alpha\neq 1$ 时, M 本身只能为非交换单群. 由于 $C_G(M)=1$, G 可视为 M 的自同构群 $\mathrm{Aut}(M)$ 的子群. 于是 G 为几乎单群. □

根据这个定理, 2 重传递群可以分成两大类. 若 2 重传递群 G 有初等交换的正则正规子群 N. 则可将 N 等同于 $GF(p)$ 上的

一个向量空间 V, 而稳定子群 G_α 就成为 V 的线性群, G 的 2 重传递性等价于 G_α 在 V 的非零向量上传递. 此时分类 G 的问题就转化成分类在非零向量集合上传递的线性群的问题. 在这个问题上主要是 Huppert 和 Hering 做了大量的研究, 并使分类问题获得解决. 若 G 为几乎单群, 则借助单群分类定理, 以及对每类单群的自同构群的了解, 可以列举出 G 的所有可能. 若 G 为一个几乎单群, 则考察它的那样的极大子群 M, 使 M 的主特征标在 G 上的诱导特征标为主特征标和一个不可约特征标的和. 用这个考虑 Kantor, Curtis 和 Seitz 解决了基柱为 Lie 型群的 2 重传递群的分类. 对交错群和散在单群, 则分情况一一加以研究, 最后决定了所有的二重传递群.

下面给出二重传递群的一览表.

(A) G 有非交换单纯正规子群 $T, T \le G \le \mathrm{Aut}(T)$. 此处列出 T 以及 G 的次数

(1) A_n, $n \geq 5$;

(2) $PSL(d,q)$, $d \geq 2$; $n = (q^d-1)/q-1$, $(d,q) \neq (2,2),(2,3)$;

(3) $PSU(3,q)$, $q > 2$; $n = q^3+1$;

(4) $Sz(q)$, $q = 2^{2e+1} > 2$; $n = q^2+1$;

(5) ${}^2G_2(q)$, $q = 3^{2e+1}$; $n = q^3+1$;

(6) $S_p(2d,2)$, $d \geq 3$; $n = 2^{2d-1} \pm 2^{d-1}$;

(7) $PSL(2,11)$; $n = 11$;

(8) M_n; $n = 11, 12, 22, 23, 24$;

(9) M_{11}; $n = 12$;

(10) A_7; $n = 15$;

(11) HS; $n = 176$;

(12) Co_3; $n = 276$;

(B) G 有 p^d 阶初等交换的正规子群 N, p 为素数. 把 N 看成 $GF(p)$ 上 d 维向量空间, G 的点稳定子群 G_0 (0 表示零向量) 或 G 有下列可能:

(1) $G \leq A\Gamma L(1,n)$;

(2) $G_0 \trianglerighteq SL(m,q)$; $q^m = p^d$;

(3) $G_0 \trianglerighteq Sp(m,q)$; $q^m = p^d$;

(4) $G_0 \trianglerighteq G_2(q)'$; $q = p^d$, q 为偶数;

(5) $G_0 \trianglerighteq A_6$ 或 A_7; $n = 2^4$;

(6) $G_0 \trianglerighteq SL(2,3)$ 或 $SL(2,5)$; $n = p^2$, 其中 $p = 5,7,11,19,23,29$ 或 59, 或 $n = 3^4$;

(7) G_0 有 2^5 阶超特殊的正规子群 E, G_0/E 同构于 S_5 的一个子群; $n = 3^4$;

(8) $G_0 = SL(2,13)$; $n = 3^6$.

在上表中，情况 (A) 中的 (1)-(6) 和 (B) 中的 (1)-(4), 代表了十个无限系列的 2-传递群. 表中其余的 2-传递群是不成系列的. 对其中的某些群，读者已经了解. 下面的例子将对另外几个常见的情形进行初步的讨论.

例 9.2 $PSU(3,q)$ 有一个级数为 q^3+1 的 2 重传递表示.

证 设 $\mathbf{F} = GF(q^2)$, $\mathbf{F}_0 = GF(q)$. 则 $\mathbf{F}$ 有一个 2 阶自同构 $\sigma: a \mapsto a^q$, $\forall a \in \mathbf{F}$, 而 $\mathbf{F}_0$ 为 σ 的不动点域. 设 V 为 $\mathbf{F}$ 上 3 维非退化的 Hermite 空间. 则在 V 中可取基 u_1, u_2, u_3 使得

$$(u_1,u_1) = (u_3,u_3) = (u_1,u_2) = (u_2,u_3) = 0,$$
$$(u_1,u_3) = (u_2,u_2) = 1.$$

此时 $SU(3,q)$ 由 V 的保持 Hermite 积不变同时行列式为 1 的线性变换组成. $G = PSU(3,q) = SU(3,q)/Z(SU(3,q))$. G 可以看成相应的 2 维射影空间的射影变换群.

令 Ω 表示 V 中的一维迷向子空间所成的集合. 我们要证明 $|\Omega| = q^3+1$, 并且 G 在 Ω 上为 2 重传递的. 以下，对 $a \in \mathbf{F}$, 我们写 $a^\sigma = \bar{a}$.

设 $v = au_1 + bu_2 + cu_3$, $a,b,c \in \mathbf{F}$, 为迷向向量. 若 $a = 0$, 则因 $(v,v) = a\bar{c} + \bar{a}c + b\bar{b} = 0$, 有 $b = 0$. 此时, $\langle v\rangle = \langle u_3\rangle$. 设 $a \neq 0$, 则在 $\langle v\rangle$ 中恰有一个向量，其第一个坐标为 1. 我们计算形如 $v = u_1 + bu_2 + cu_3$ 的迷向向量的个数. 此时 $(v,v) = c + \bar{c} + b\bar{b} = 0$.

由于对取定的 $b\in\mathbf{F}$, 方程 $c+\overline{c}=-b\overline{b}$ 恰有 q 个解，故而 V 中正好有 q^3 个一维迷向子空间，其生成元的第一个坐标不为 0. 因此 $|\Omega|=1+q^3$.

由 Witt 引理知 G 在 Ω 上传递. $SU(3,q)$ 中的保持 $\langle u_3\rangle$ 不动的线性变换形如

$$g=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix},$$

因为 g 保持向量间 Hermite 积不变，且 $\det g=1$, 我们有

$$a_{21}=0,\ a_{22}\overline{a_{22}}=1,$$

$$a_{11}\overline{a_{33}}=1.\ a_{11}\overline{a_{13}}+\overline{a_{11}}a_{13}+a_{12}\overline{a_{12}}=0$$

$$a_{11}\overline{a_{23}}+a_{12}\overline{a_{22}}=0,\ a_{11}a_{22}a_{33}=0.$$

全部这样的变换组成 $SU(3,q)$ 的一个子群，它在 $PSU(3,q)$ 中的像 H 为 $\langle u_3\rangle$ 在 G 中的稳定子群. 更进一步，集合

$$\left\{\begin{pmatrix} 1 & x & y \\ & 1 & -\overline{x} \\ & & 1 \end{pmatrix}\ \middle|\ x\overline{x}+y+\overline{y}=0\right\}$$

也组成 $SU(3,q)$ 的子群，它在 G 中的像是 L, 为 H 的子群，即 L 也使 $\langle u_3\rangle$ 不变. 但由于

$$(1,0,0)\begin{pmatrix} 1 & x & y \\ & 1 & -\overline{x} \\ & & 1 \end{pmatrix}=(1,x,y),$$

所以 L 在 $\Omega-\langle u_3\rangle$ 上传递. 于是 $H=G_{\langle u_3\rangle}$ 在 $\Omega-\langle u_3\rangle$ 上传递，而 G 在 Ω 上 2-传递. □

例 9.3 M_{11} 有一个 660 阶子群，进而 M_{11} 可以忠实地表示成为 12 级 3-传递群.

证 仍使用 §7 中的记号， $M_{11} = H = \langle u, a, b, x, y\rangle$, 其中

$$u = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9),$$

$$a = (2\ 3\ 4\ 7)(5\ 6\ 9\ 8),$$

$$b = (2\ 5\ 3\ 9)(4\ 8\ 7\ 6),$$

$$x = (1\ 10)(4\ 5)(6\ 8)(7\ 9),$$

$$y = (10\ 11)(4\ 7)(5\ 8)(6\ 9),$$

仍记 $v = u^a = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$. 令 $\widehat{H} = \langle v, x, y\rangle$. 我们分几步证明结论，

第一步令 $\widehat{L} = \langle v, x\rangle$, 则 $\widehat{L} \cong A_5$.

实际上 $vx = (1\ 5\ 6\ 7\ 10)(2\ 4\ 9\ 3\ 8)$. 所以 $v^3 = x^2 = (vx)^5 = 1$. 于是 $\widehat{L} \cong A_5$.

第二步，下列元素属于 $\widehat{L}$:

$$l_1 = (1\ 6\ 10\ 5\ 7)(2\ 9\ 8\ 4\ 3)$$

$$l_2 = (1\ 4\ 9\ 10\ 8)(2\ 7\ 6\ 5\ 3)$$

$$l_3 = (1\ 7\ 8)(2\ 4\ 5)(6\ 9\ 10)$$

$$k = (2\ 3)(4\ 7)(5\ 9)(6\ 8).$$

实际上， $l_1 = (vx)^2$, $l_2 = (xv)^2$. 又令

$$g = l_2^3 l_1^4 = (1\ 6\ 3)(2\ 10\ 8)(4\ 9\ 7),$$

则 $k = x^g$ 而 $l_3 = l_2 k$. 这证明这些元素都属于 $\widehat{L}$.

第三步，令 $\widehat{K} = \langle v, k\rangle$, 则 $\widehat{L} = \widehat{K} \cup \widehat{K}x\widehat{K} \cup \widehat{K}l_1\widehat{K}$.

显然 $\widehat{K} \leq (\widehat{L})_{10}$, $|\widehat{K}| = 6$, 且 $\widehat{K}$ 在 $\{1, 2, \cdots, 10\}$ 上有三个轨道 $\{10\}$, $\{1, 4, 7\}$, $\{2, 3, 5, 6, 8, 9\}$. 而 $10^x = 1$, $10^{l_1} = 5$. 因而得 $\widehat{K} = (\widehat{L})_{10}$, $\widehat{L}$ 在 $\{1, 2, \cdots, 10\}$ 上为秩 3 本原群，并有上述分解.

第四步. $\widehat{H} = \langle \widehat{L}, y\rangle$ 为 660 阶群：

我们证明 $\widehat{H}$ 为 $\widehat{L}$ 的传递扩张. 令

$$X = \widehat{L} \cup \widehat{L}y\widehat{L},$$

而证明 X 对乘法封闭. 这只需证 $y\widehat{L}y \leq X$. 容易验证 $\widehat{K}^y = \widehat{K}$, 且 $yxy = xyx$, $yl_1y = l_3yl_2$. 所以 $y\widehat{K}y = \widehat{K}$, $y\widehat{K}x\widehat{K}y = \widehat{K}yxy\widehat{K} = \widehat{K}xyx\widehat{K} \leq \widehat{L}y\widehat{L}$, $y\widehat{K}l_1\widehat{K}y = \widehat{K}yl_1y\widehat{K} = \widehat{K}l_3yl_2\widehat{K} \leq \widehat{L}y\widehat{L}$. 故 X 为一个子群, 因之 $X = \widehat{H}$. 这样一来, $\widehat{L}$ 为点 "11" 在 $\widehat{H}$ 中稳定子群. $|\widehat{H}| = 660$.

第五步 M_{11} 可表示成 12 级 3-传递群.

用 Ω 表示 $\widehat{H}$ 在 H 内右陪集的集合, 则 $|\Omega| = 12$. 因 $H = M_{11}$ 为单群, H 可忠实地表示成 Ω 上传递群. 因 $11 \mid |M_{11}|$. 所以 H 在 Ω 上 2-传递. 若 $\alpha, \beta \in \Omega$, 则 $|H_{\alpha\beta}| = 60$. $H_{\alpha\beta}$ 中的 5 阶元在 $\Omega - \{\alpha, \beta\}$ 上有两个 5 长的轨道. 若 $H_{\alpha\beta}$ 在 $\Omega - \{\alpha, \beta\}$ 上不传递, 由习题 8 知 $|H_\alpha|$ 为奇数, 与 $|H_\alpha| = 660$ 矛盾. 这证明了 $H_{\alpha\beta}$ 在 $\Omega - \{\alpha, \beta\}$ 上传递, 而 H 在 Ω 上 3-传递.

注: H 中的 660 阶子群 $\widehat{H}$ 同构于 $PSL(2, 11)$. □

例 9.4 A_7 可以表示成 15 级的 2 重传递群.

证 在例 6.6 中我们看到 S_7 中有一个极大子群 $H \cong PSL(2, 7)$. 因为 $H < G = A_7$, 用 Ω 表示 H 在 G 中的右陪集全体, 那么 G 可表成 Ω 上的本原群, 其中 $|\Omega| = |G : H| = 15$. 由于 $7 \mid |G|$, G 的 Sylow7-子群在 Ω 上有一个不动点和两个长为 7 的轨道. 如果 G 在 Ω 上非 2-传递, 则 G 在 Ω 上的秩为 3, 而且次级数为 $1, 7, 7$, 均为奇数. 这只有 $|G|$ 为奇数时才有可能. 因此 G 在 Ω 上为 2-传递群. □

例 9.5 存在 16 级的 2 重传递群, 其点稳定子群与 A_6, S_6 或 A_7 同构.

证 我们利用同构 $H = GL(4, 2) \cong A_8$, 于是在 $GL(4, 2)$ 中有子群 X, Y, Z 使 $X \cong A_7$, $Y \cong A_6$, $Z \cong S_6$, 视 $GL(4, 2)$ 为 $GF(2)$ 上 4 维向量空间 V 的自同构群. 则 $GL(4, 2)$ 在 V 的非零向量上传

递. 因为 V 中共有 15 个非零向量，而 $|H:X|=8$, $|X:Y|=7$, 所以 X,Y,Z 在 V 的非零向量上传递. 另一方面，若 T 表示 V 的平移群，而 $L\le GL(4,2)$ 为在 V 的非零向量上传递的子群. 那么 $T\rtimes L$ 为在向量集合上 2-传递. 这完成了我们的证明. □

除上述例子外. 在习题中. 我们会看到另外几个 2-传递群.

习　题

1. 给定生成元 a,b, 求 $G=\langle a,b\rangle$ 以及稳定子群 G_1.

(1) $a=(2\ 9\ 13\ 6)(3\ 4\ 12\ 11)(5\ 7\ 10\ 8)$,

$b=(1\ 5)(2\ 4)(6\ 13)(7\ 12)(8\ 11)(9\ 10)$.

(2) $a=(1\ 2)(3\ 4)(5\ 6)(7\ 8)$, $b=(2\ 3\ 5\ 4\ 7\ 8\ 6)$.

2. 写出 S_{12} 的全部非传递的和非本原的极大子群.

3. G 为 Ω 上传递的非本原群. $\{\Delta_i\}$ 为非本原系. 则 G 作用于集合 $\{\Delta_i\}$ 上. 求作用的核 K. 举例说明此时可能 $K=1$, 也可能 $K\neq 1$. 当 $K\neq 1$ 时, $K^{\Delta_i}\cong K^{\Delta_j}$, $\forall i\neq j$.

4. 如果本原群 G 的级数 >2 为偶数，则 G 的阶为 4 的倍数.

5. 设 G 为 Ω 上传递群，Δ,Ψ 均为 G 的块. 则 $\Delta\cap\Psi$ 也是 G 的块.

6. 构造一个 9 级置换群 G, 使 $|G|=27$, 但 G 中没有 9 阶元.

7. 设 G 为 Ω 上置换群，$\alpha\in\Omega$, p 为素数. 若 p^m 为 $|\alpha^G|$ 的因子, P 是 G 的一个 Sylow p-子群，那么 p^m 也是 $|\alpha^P|$ 的因子.

8. 置换群的阶为奇数当且仅当 G 的所有传递成分的级数以及所有的 G_α $(\alpha\in\Omega)$ 的轨道的级数均为奇数.

9. 设 G 为 Ω 上本原群，$x\in G$, x 为 s 个长 >1 的轮换的乘积，且 x 的级数为 m. 证明 G 的秩不超过 $m-s+1$.

10. $m\ge 5$, S_m 可以表示成为 $\{1,2,\cdots,m\}$ 的二元子集上的本原群. 证明其最小级数为 $2m-4$.

11. 设 G 为 Ω 上本原群, 其阶 $|G|$ 为复合数. 设 $\Gamma,\Delta\subset\Omega$, $|\Gamma|=|\Delta|>0$, 并设 α,β 为 Ω 中两个不同的点，那么 G 包含一个元素 g, 使 $\alpha^g\in\Gamma$ 而 $\beta^g\notin\Delta$.

12. (1) 设 $g=(\alpha\ \beta_1\ \cdots\ \beta_s)$, $h=(\alpha\ \gamma_1\ \cdots\ \gamma_t)$, 其中 $\{\beta_1,\cdots,\beta_s\}\cap\{\gamma_1,\cdots,\gamma_t\}=\varnothing$. 则 $[g,h]$ 为 3-轮换.

(2) 设 G 为 Ω 上本原群且 $G\not\geq A_\Omega$. 则

$$|G|<\frac{n!}{[\frac{n+1}{2}]!},\ \text{其中 } n=|\Omega|.$$

13. 证明定理 4.10.

14. 设本原群 G 有一个次轨道长为素数 p. 证明 G 的稳定子群 $G_\alpha(\alpha \in \Omega)$ 的阶 $|G_\alpha|$ 不能被 p^2 整除.

15. G 为 Ω 上传递群, K 为一个共轭类. 设 $x \in K, \alpha \in \Omega$, 则 x 的不动点个数为

$$|\text{fix }_\Omega(x)| = \frac{|G_\alpha \cap K||\Omega|}{|K|}.$$

16. 设 G 为 Ω 上传递群, $H = G_\alpha, \alpha \in \Omega$. 设 G 中仅有一个对合的共轭类, 其中每个对合为 N 个对换的乘积. 对每个非平凡的自配对轨道 Δ, 若 $(\alpha\ \beta) \in \Delta$, $\text{inv}(\Delta)$ 表示其轮换分解中有对换 $(\alpha\ \beta)$ 的对合的个数, 则

$$N = \frac{c}{2|H|}\sum |\Delta(\alpha)| \cdot |\text{inv}(\Delta)|,$$

其中 c 为对合的中心化子的阶.

17. 令 $G = PSL(2,19)$, H 为 G 中同构于 S_4 的极大子群. G 表示成为 H 的右陪集集合上的置换群. 求此时 G 的秩, 次级数以及自配对次轨道的级数.

18. 证明命题 5.11.

19. 设 T 为非交换单群, $X = \{(a_1, a_2, \cdots, a_m) \mid a_i \in T\}$ 为同构于 T^m 的群, $T_i = \{1, \cdots, 1, a_i, 1, \cdots, 1) \mid a_i \in T\}$, π_i 为 X 到 T_i 的射影, $D < X$ 为子群. 若对一切的 i, $1 \le i \le m$, $\pi_i(D) = T_i$, $\pi_i|_D$ 的核与 $\pi_1|_D$ 的核相同. 则对一切的 i, 有 T_1 到 T_i 的同构 φ_i 使

$$(a_1, a_2, \cdots, a_m) \in D \iff a_i = a_1^{\varphi_i},\ \forall i \in \{1, 2, \cdots, m\}.$$

20. 设 G 为 n 级本原群, $n \ge 9$. 证明若 G 包含一个级数为 4 的 2 阶元素, 则 $G \ge A_n$.

21. 决定所有 8 级本原群. 结合习题 2, 决定 S_8 的所有极大子群.

22. 证明 20 级本原群一定是 2-传递群.

23. 证明 168 阶单群, 660 阶单群在同构意义下都只有一个.

24. 设 $\mathcal{D}$ 为一个 5-$(24,8,1)$ 设计. 设 $B = \{y_1, \cdots, y_8\}$ 为一个区组. 对任意的 k, $k = 0,1,2,3,4$, 计算 $b, r, \lambda_1, \lambda_2, \lambda_3, \lambda_4$. 计算与 B 的交为事先指定的 $k(0 \le k \le 4)$ 个点的区组的个数. 证明 $\mathcal{D}$ 中任意两个区组交于偶数个点.

25. 设 $\mathcal{D}$ 为一个 5-$(24,8,1)$ 设计, 设 x_1, x_2, x_3 为三个点. 证明 $\mathcal{D}_{x_1,x_2,x_3}$ 为一个 2-$(21,5,1)$ 设计, 它正好是一个 4 阶射影平面.

26. 每个级数为 n 的传递群当中有一个 n 级的元素.

27. 设 G 为 Ω 上传递群, 用 $\pi(x)$ 表示元素 x 的不动点个数, $\delta(x)$ 表示元素 x 的轮换分解式中对换的个数. 则

(1) 若 G 为 2-传递的，则 $\sum_{x\in G}\delta(x)=\frac{|G|}{2}$，

(2) 若 G 为 3-传递的，则 $\sum_{x\in G}\delta(x)\pi(x)=\frac{|G|}{2}$.

28. 用 $0,1,2,3,4$ 表示 $\mathbf{F}=GF(5)$ 中的元素，(加，乘按模 5 的加法和乘法进行.) 在 $G=GL(2,5)$ 中取两个元素

$$a=\begin{pmatrix} & 4\\ 1 & \end{pmatrix},\ b=\begin{pmatrix}1 & 3\\ 4 & 3\end{pmatrix}.$$

求 $H=\langle a,b\rangle$ 的阶和 H 的合成因子. 证明 H 传递地作用于 $\mathbf{F}$ 上 2 维空间的非零向量上，求此时 H 的次级数，由此构造一个 25 级 2 重传递群.

29. 给定 $\mathbf{F}=GF(7)$ 上的矩阵

$$a=\begin{pmatrix} & 6\\ 1 & \end{pmatrix},\ b=\begin{pmatrix}1 & 3\\ 6 & 5\end{pmatrix}.$$

求 $H=\langle a,b\rangle$ 的阶和 H 的合成因子. 由此构造一个 49 级 2 重传递群.

30. $|\Omega|=11$. G 为 Ω 上 4 重传递群. 若 $G\not\geq A_\Omega$, 则 G 与 M_{11} 置换同构.

31. 设 G 有一个正则正规子群 N. 则

(1) 若 G 在 Ω 上 2-传递，则 $|N|=p^a$ 为素数方幂.

(2) 若 G 在 Ω 上 3-传递，则 $|N|=4$.

32. 设 G 为 Ω 上 k 重传递群 $(k\geq 1)$, $1\neq N\trianglelefteq G$. 则 N 或为正则群，或为精确 $k-1$ 重传递群，或为 $(k-\frac{1}{2})$ 重传递群.

33. 证明 A_7 中包含 30 个 168 阶本原群，它们在 S_7 下相互共轭，而在 A_7 下组成两个长度为 15 的共轭类.

34. 在 A_8 中有一个阶为 $8\cdot 168=1344$ 的本原群 G, G 的点稳定子群为 168 阶单群. 证明 G 中包含一个传递子群，它也是 168 阶单群.

第 XIII 章

群的几何理论

近年来，群的几何理论发展十分迅速．这些理论大多起源于 Tits 的 *厦* (building) 与 BN-对 (BN-pair) 理论．厦与 BN-对概念的产生，最早可追溯至本世纪 50 年代．当时 Tits 为了对半单 Lie 群，特别是例外 Lie 群，给出一个统一的几何刻划，首先提出了厦与 BN-对的概念．随着有限单群分类工作的进行，这一理论日益受到群论学者注意，它对 Lie 型单群 (simple groups of Lie type) 的识别起了重要作用． 1980 年有限单群分类定理完成，厦与 BN-对的研究工作进入了新的阶段．自 70 年代以来，厦与 BN-对理论有许多重要的推广，这些理论和方法渗透到许多代数学分支中去，成为研究这些学科的重要工具．特别在有限群领域中它们起到了举足轻重的作用．除上文中所提到的 Lie 型单群理论外，对于诸如 *零散单群* (sporadic simple group) 理论，单群分类定理的简化，群表示论等等，它们均已成为不可缺少的工具．这些推广本身也发展成一些十分活跃的数学分支，其共同特点是都带有较强的组合色彩．因此 Aschbacher 把这些理论统称为几何组合论，其中包括：射影几何，(广义的) Tits 几何；某些图；(抽象) 单式复形．他还指出，所有上述理论均可纳入最后两类的范畴．本章我们着重介绍 Tits 几何理论．本章分为六节： §1 介绍 *复形* (complex) 的基本概念； §2 介绍一种特殊的复形： Coxeter *复形*; §3 为厦理论； §4 为 Tits 系和 BN-对理论； §5 为 *融合* 理论； §6 的内容，实际上并不属于本章标题所限定的内容，而是本书部分内容的一

个归纳：有限单群及其分类.

对一般的群几何理论感兴趣的读者，可参阅以下著作：

J. Tits, *Bildings of spherical type and finite BN-pairs*, Springer-Verlag, LNM 386(1974).

A. Dold & B. Eckman, *Buildings and the geometry of diagrams*, Springer-Verlag, LNM 1181(1984).

对融合理论感兴趣的读者，请参阅下列教材：

H.Kurzweil & B.Stellmacher, *Theorie der endlichen Gruppen*, Springer-Verlag (1998).

§1. 复形

本节我们讨论复形的性质和结构.

定义 1.1 令 I 为一集合. $\Delta=(V,\tau,\mathcal{S},I)$ 说是集合 I 上的 **复形**, 其中 V 为一集合； $\mathcal{S}$ 为 V 的某些子集之集合，通常我们把 Δ 和 $\mathcal{S}$ 等同起来： $A\in\mathcal{S}$ 也记作 $A\in\Delta$; τ 为 V 到 I 的映射，叫做 Δ 上的 **型** (type) 映射, 且 $\tau:A\to I,\forall A\in\Delta$ 为单射， A^τ 说是 A 的型，又 $\forall x\in V$, x^τ 说是 x 的型. Δ 上定义了序关系 $\subset$, 若 $A\subset B$, 则说 A 包含于 B 中，或者说 A 是 B 的 **面** (face). 若 $A\in\mathcal{S}$, 则 A 中所有的面均属于 $\mathcal{S}$, 且 A 连同其中所有的面同构于一个集合的幂集合. 又若 $A,B\in\mathcal{S}$, 则 A,B 在 $\mathcal{S}$ 中有极大下界，记作 $A\cap B$; $\mathcal{S}$ 中的元也叫做 **单形** (simplex).

任一复形都包含一最小元，记作 0. 注意对于复形中的包含关系, 我们还采用记法 "$\supset$", 读作 "包含": 若 $A\subset B$, 也可记作 $B\supset A$. 有时为了表明复形 Δ 的包含关系为 $\subset$, 也将 Δ 写作 $(\Delta,\subset)$.

若 $A\in\Delta$, 则 $|A^\tau|$ 叫做 A 的 **秩**(rank), 记作 $\mathrm{rk}\ A$. 极小非零元本身之秩为 1, 并称为 Δ 的 **顶点** (vertex). Δ 中极大元的秩不超过 $|I|$. 规定复形 Δ 的秩为 $\mathrm{rk}\ \Delta=\sup\{\mathrm{rk}\ A\mid A\in\mathcal{S}\}$.

$\Delta'=(V',\tau',\mathcal{S}',I)$ 说是复形 $\Delta=(V,\tau,\mathcal{S},I)$ 的一个 **子复形** (subcomplex), 若 $V'\subset V$, Δ' 上的序关系由 Δ 的序关系导出， τ'

为 τ 在 V' 上的限制; 且若 $A \in \Delta'$, 则 A 的属于 Δ 的一切面均属于 Δ'.

下列命题可直接由定义得出.

命题 1.2 设 $(\Delta, \subset)$ 为一复形, $A \in \Delta$, 则 Δ 中全体包含 A 的元素, 连同由 $\subset$ 所导出的包含关系, 构成一个复形. 这一复形叫做 A 的 星 (star), 记作 st A. 若 $B \in$ st A, 则 B 在 st A 中的秩叫做 A 在 B 中的 余维数 (codimension), 记作 $\operatorname{codim}_B A$. 在 B 固定的情况下 $\operatorname{codim}_B A$ 也简记为 codim A.

定义 1.3 I 上复形 $\Delta = (V, \tau, \mathcal{S}, I)$ 说是一个 室复形 (chamber complex), 若 Δ 中包含型为 I 的极大元 (这样的极大元叫做 室 (chamber)), 又 $\mathcal{S}$ 中每个元都包含在一个室中; 且对于任意给定的二个室 C, C', 存在有限室序列

$$C = C_0, C_1, \cdots, C_m = C'$$

使得

$$\operatorname{codim}_{C_{i-1}}(C_{i-1} \cap C_i) = \operatorname{codim}_{C_i}(C_{i-1} \cap C_i) \leq 1, \qquad (1.1)$$

其中 $i = 1, \cdots, m$, 这时 Δ 说是连通的 (connected).

定义 1.4 复形 $\Delta = (V, \tau, \mathcal{S}, I)$ 到复形 $\Delta' = (V, \tau', \mathcal{S}', I)$ 的映射 α 说是 Δ 到 Δ' 的 态射 (morphism), 若 α 保持 Δ 中元的包含关系, 且 $\forall A \in \Delta$, $A^{\tau} = (A^{\alpha})^{\tau'}$.

由定义 1.4 可知, A 的面集合与 A^{τ} 的面集合成 1-1 对应.

我们还可定义复形间的满态射, 单态射, 同构, 自态射及自同构等等.

由下列命题我们看到, 群与复形有着非常密切的关系.

命题 1.5 设 I 为一集合. 令 G 为一群, $\mathcal{F} = \{G_i \mid i \in I\}$ 为 G 的一个子群集. 我们定义复形 $\Delta(G, \mathcal{F}) = (V, \tau, \mathcal{S}, I)$ 如下: 对

于 $J \subseteq I$, 定义 $S_J = \bigcap_{i \notin J} G_i$, 特别地, $S_{I \setminus \{i\}} = G_i$, $S_\varnothing = \bigcap_{i \in I} G_i$. 令 $V = \{G_i x \mid i \in I, x \in G\}$, $\mathcal{S} = \{S_J x \mid J \subseteq I, x \in G\}$, $\tau : S_J x \mapsto I \setminus J$. 在 Δ 上定义序关系 "$\supset$": 规定 $S_J x \supset S_K y$, 如果 $J \subseteq K$, 且陪集 $S_J x$ 包含陪集 $S_K y$.

$\Delta(G, \mathcal{F})$ 说是群 G 关于子群集合 $\mathcal{F}$ 的陪集复形.

对于陪集复形 $\Delta = \Delta(G, \mathcal{F})$, 成立

(1) G 通过右乘作用在 Δ 上, 这时 $G \le \mathrm{Aut}(\Gamma)$.

(2) G 在 Δ 中所有型为 $J, J \subset I$, 的复形集合上传递.

(3) S_J 为型为 J 的单形 S_J 在 G 中的稳定子.

(4) Δ 为室复形, 当且仅当 $G = \langle G_i \mid i \in I \rangle$.

本命题的证明作为练习留给读者.

下文中, 除非有特殊说明, 我们所考虑的复形全部都是室复形. 我们以 Cham Δ 表示 Δ 中室的集合. 对于 $C, C' \in$ Cham Δ, 序列 $\mathbf{G} = (C = C_0, C_1 \cdots, C_m = C')$ 叫做连接 C 和 C' 长为 m 的廊 (gallery), 若对任意 i, 成立

$$\mathrm{codim}\ _{C_{i-1}}(C_{i-1} \cap C_i) = \mathrm{codim}\ _{C_i}(C_{i-1} \cap C_i) = 1.$$

设 $C, D \in$ Cham Δ 且 $\mathrm{codim}\ _C(C \cap D) = \mathrm{codim}\ _D(C \cap D) = 1$, 则说 C 和 D 相邻 (adjacent), $W = C \cap D$ 叫做一个 墙 (wall). 若 $A, A' \in \Delta$, 则连接包含 A 的室与包含 A' 的室并具有最短长度的廊之长, 叫做 A 与 A' 间的 距离, 记作 dist AA'. 由此易知室 C 与室 C' 相邻当且仅当 dist $CC' = 1$. 廊 $\mathbf{G}$ 说是 萎缩的 (stammer), 若有 $i \in \{0, 1, \cdots, m-1\}$ 能使 $C_{i+1} = C_i$.

定义 1.6 一个室复形说是 薄的 (thin), 若它的每个墙都恰包含在两个室之中. 一个室复形说是 厚的 (thick), 若其中每个墙都包含在至少三个室之中.

易知, 室复形间的态射把任意廊仍映到廊, 且廊的像的长度不超过原来的廊的长度.

下面我们给出一个重要的室复形的例子.

例 1.7 令 V 为域 $\mathbf{F}$ 上 $d+1$ 维向量空间，$\mathcal{P}$ 为 V 上射影空间，这时 $\dim \mathcal{P}=d$. 我们利用 $\mathcal{P}$ 的子空间序列之集合构造一个室复形. (与射影空间 $\mathcal{P}$ 有关的性质请参阅第 XI 章，§3.)

以 $\mathcal{M}$ 表示 $\mathcal{P}$ 中全体非空真子空间之集合. $\mathcal{M}$ 中元素 $\alpha_i, i=1,\cdots,k$ 的序列

$$A:\alpha_1\supset\cdots\supset\alpha_k$$

叫做一个 k 秩旗 (flag). 实际上，旗 A 也可以看做是 $\mathcal{M}$ 中特别选定的子集合. 令 B 为 $\mathcal{P}$ 中另一旗，若 B 中任一项都是 A 中的项，则说 A 是 B 的一个加细 (refinement), 并说 A 包含 B, 记作 $B\subset A$. 由 $\mathcal{P}$ 中所有旗构成的集合 $\mathcal{F}$ 对于以上定义的包含关系 "$\subset$" 构成一个偏序集，叫做关于 $\mathcal{P}$ 的 **旗空间**(flag space). 令 Σ 为射影空间 $\mathcal{P}$ 的一个框架，

$$A:\alpha_1\supset\alpha_2\supset\cdots\supset\alpha_k$$

为 $\mathcal{P}$ 中一个旗. 若对任意 α_i 都可以找到 Σ 的子集 Σ_i, 使得 α_i 由 Σ_i 中的点所张成，则说框架 Σ 支撑了旗 A. 对于固定的框架 Σ, 我们以 Σ_Δ 或仍以 Σ 表示由 Σ 所支撑的全体旗之集合. 我们还以 $\mathcal{M}_\Sigma$ 表示由 Σ 的子集所张成的非空真子空间之集合.

我们有如下的:

定理 1.8 设 $\mathcal{P}$ 为一 d 维射影空间，$\mathcal{M},\Sigma$ 及 $\mathcal{F}$ 如以上所定义. 令 $I=\{0,\cdots,d-1\}$, 定义

$$\tau:\mathcal{M}\to I$$

如下：对于 $\alpha\in\mathcal{M}$ 规定 $\alpha^\tau=\dim\alpha$. 则

(1) 任一 $\Sigma_\Delta=(\mathcal{M}_\Sigma,\tau,\Sigma,I)$ 为 I 上薄室复形，

(2)$\Delta(\mathcal{P})=(\mathcal{M},\tau,\mathcal{F},I)$ 为 I 上厚室复形.

在证明这一定理之前先证下述引理.

引理 1.9 令 A 和 B 为 $\Delta(\mathcal{P})$ 中任意二个旗，则有 Σ 同时包含 A 和 B.

证 对 $\mathcal{P}$ 的维数施行归纳.

不失一般性, 可假定 A 和 B 都是 $\Delta(\mathcal{P})$ 的极大旗. 设

$$A:\alpha_1\supset\alpha_2\supset\cdots\supset\alpha_d,\quad B:\beta_1\supset\beta_2\supset\cdots\supset\beta_d.$$

令 k 为能使 $\beta_k\not\subseteq\alpha_1$ 的最大整数. 若 $\beta_1=\alpha_1$, 则令 $k=0$, 且 $\beta_0=\mathcal{P}$. 规定: $\gamma_{i+1}=\alpha_1\cap\beta_i(i<k),\gamma_j=\beta_j(j>k)$.

易知: $\dim\gamma_{i+1}=\dim\beta_i-1,(i<k)$. 则 $A_1:\alpha_2\supset\cdots\supset\alpha_d$ 及 $C:\gamma_2\supset\cdots\supset\gamma_d$ 均为射影空间 α_1 的极大旗. 由归纳假定, 有 α_1 的框架 Σ_1 同时支撑 A_1 和 C. 由定义 $\beta_i=\gamma_{i+1}\cup\beta_k$, 这里 $i\le k$. 令 $\Sigma=\{\Sigma_1,P\}$, 其中 $P\in\beta_k\setminus\beta_{k+1}$, 从而 $A,B\in\Sigma_\Delta$. 这就证明了引理. □

定理 1.8 之证明: 我们可以很容易地验证, Σ_Δ 为一室复形.

首先我们注意到, $C:\delta_1\supset\delta_2\supset\cdots\supset\delta_{d-1}$ 为 Σ_Δ 中一个极大元, 其中 δ_i 均由 Σ 所支撑, 特别地 $C^\tau=I$.

下面我们证明: 若 $A:\alpha_1\supset\cdots\supset\alpha_k$ 为 Σ_Δ 中任一旗, 则 A 包含在 Σ_Δ 的一个极大旗之中. 由假定, 每一 α_i 都由 Σ 的某一子集 Σ_i 张成. 则 $\dim\alpha_i\le|\Sigma_i|-1$. 又因 Σ 中的点互相无关, 从而 $|\Sigma_i|\le|\alpha_i\cap\Sigma|\le\dim\alpha_i+1$. 由上可得 $\dim\alpha_i=|\Sigma_i|-1$, $\alpha_i\cap\Sigma=\Sigma_i$. 故相应于 A, 有 Σ 的子集序列: $\Sigma_1\supset\cdots\supset\Sigma_k$, 其中 $\Sigma_i\ne\Sigma_{i+1}$ 且 Σ_i 张成 α_i. 由线性代数可知, 存在 Σ 的子集序列: $\Sigma^{(1)}\supset\cdots\supset\Sigma^{(d)}$, 其中 $\Sigma^{(i)}\ne\Sigma^{(j)},i\ne j$, 能使每个 Σ_i 都等于某一 $\Sigma^{(k_i)}$.

令 β_k 为由 $\Sigma^{(k)}$ 中点张成的子空间, 便得到一个旗 $B:\beta_1\supset\beta_2\supset\cdots\supset\beta_d$, B 为一包含 A 的极大旗.

以下再证 Σ_Δ 为连通的. 为此, 对维数 d 进行归纳. 令 $A,B\in\Sigma_\Delta$. 不妨假定 A 和 B 都是 Σ_Δ 中极大旗, 即

$$A:\ \alpha_1\supset\cdots\supset\alpha_d$$

$$B:\ \beta_1\supset\cdots\supset\beta_d.$$

首先假定 $\alpha_1=\beta_1$, 则 α_1 连同包含在 α_1 中的子空间构成了一个 $d-1$ 维射影空间 $\mathcal{P}_1$. 集合 $\Sigma_1=\Sigma\cap\alpha_1$ 为 $\mathcal{P}_1$ 的一个框架,

且下列二旗：

$$A_1: \quad \alpha_2 \supset \cdots \supset \alpha_d$$
$$B_1: \quad \beta_2 \supset \cdots \supset \beta_d$$

均由 Σ_1 所支撑. 由归纳假定, A_1 和 B_1 在 $\{\Sigma_1\}_\Delta$ 中连通. $\mathcal{P}_1$ 的一个极大旗. 添上 α_1, 便得到 Σ_Δ 中一个极大旗, 故 A 和 B 在 Σ_Δ 中是连通的.

现讨论 $\alpha_1 \neq \beta_1$ 的情况. 这时 Σ 中有唯一的一个点不属于 α_1 而属于 β_1, 反之亦成立. 则 $A_2: \alpha_1 \supset \alpha_1 \cap \beta_1$ 及 $B_2: \beta_1 \supset \alpha_1 \cap \beta_1$ 都属于 Σ_Δ, 故可找到 Σ_Δ 中包含 A_2 的极大旗 C. 我们有:

$$C: \alpha_1 \supset \alpha_1 \cap \beta_1 = \gamma_1 \supset \gamma_2 \cdots \supset \gamma_{d-1},$$

其中 γ_i 的定义同引理 1.9 的证明. 定义 $D: \beta_1 \supset \gamma_1 \supset \cdots \supset \gamma_{d-1}$. D 也为 Σ_Δ 中一个极大元, 且 C 和 D 相邻. 而由上述讨论知, A 和 C 连通, B 和 D 连通, 从而 A 和 B 连通.

以下证明 Σ_Δ 为薄的. 令 $A: \alpha_1 \supset \cdots \supset \alpha_{d-1}$ 为 Σ_Δ 中一秩为 $d-1$ 的旗, $\alpha_0 = \mathcal{P}$, 而 $\alpha_d = \varnothing$. 除了某一 k 之外, 所有的 $\alpha_{i-1} \setminus \alpha_i$ 都恰包含 Σ 中一个点, 而 $\alpha_{k-1} \setminus \alpha_k$ 恰包含 Σ 中二个点 P 和 Q. 令 $\alpha_k' = \alpha_k \cup \{P\}, \alpha_k'' = \alpha_k \cup \{Q\}$, 则

$$A': \alpha_1 \supset \cdots \supset \alpha_{k-1} \supset \alpha_k' \supset \alpha_k \supset \cdots,$$

$$A'': \alpha_1 \supset \cdots \supset \alpha_{k-1} \supset \alpha_k'' \supset \alpha_k \supset \cdots$$

是 Σ_Δ 中仅有的包含 A 的两个极大旗. 故 Σ_Δ 为薄的. 这就证明了 (1).

下面我们证明 $\Delta(\mathcal{P})$ 为一厚室复形. 它的连通性可由 Σ_Δ 的连通性得出. 由于 Σ_Δ 为室复形, 则 $\Delta(\mathcal{P})$ 也为室复形. 注意, 根据上文中记法, 令对应于 α_k 的子空间为 U_k, 对应于 α_{k-1} 的子空间为 U_{k-1}. 若 $W \subseteq U$, 我们把 $\dim U - \dim W$ 叫做 W 关于 U 的余维数. U_k 关于 U_{k-1} 的余维数为 2, 故 U_k 至少包含 3 个关于 U_{k-1} 余维数为 1 的子空间, 从而 $\Delta(\mathcal{P})$ 为 d 秩厚复形. 即 (2) 成立. □

在习题 5 中我们将进一步讨论 $\Delta(\mathcal{P})$ 的性质.

§2. Coxeter 系和 Coxeter 复形

Coxeter 群是十分重要的群类, Coxeter 复形是 Coxeter 群的几何实现. Coxeter 群的研究工作是 Lie 型群识别工作的关键步骤.

定义 2.1 令 $I=\{1,2,\cdots,n\}$, 矩阵 $M=(m_{ij})_{i,j\in I}$ 说是定义在 I 上的 Coxeter 矩阵, 若 M 对称, 其中 m_{ij} 为非负整数, $m_{ii}=1, m_{ij}\geq 2$.

本节下文中, 我们将用到一些关于图的概念, 如图的顶点, 图中的道路等. 这些概念均可在第 XIV 章中查到.

为方便起见, 我们常以 D-图 (diagram) 表示 Coxeter 矩阵 M: 以 I 中元作为 D-图的顶点, 顶点 i,j 以 $m_{ij}-2$ 条边相连, 或以一条边相连, 并在该边上方标以 $m_{ij}-2$. 注意, 若 $m_{ij}=2$, 则不论采取上述任一种记法, 顶点 i 和 j 间都没有边相连. Coxeter 矩阵所对应的 D-图也叫做 Coxeter 图.

例 2.2 以下矩阵

$$M=\begin{pmatrix}1&3&2\\3&1&5\\2&5&1\end{pmatrix}$$

为一 Coxeter 矩阵, M 所对应的 D-图为:

1 2 3

或

3

1 2 3

定义 2.3 令 $M=(m_{ij})_{i,j\in I}$ 为集合 I 上的 Coxeter 矩阵. 二元组 (W,S) 说是一个型为 M 的 Coxeter 系, 若下列条件成立:

(1) $S=\{s_i \mid i\in I\}$, 其中 $o(s_i)=2,\ \forall i\in I$;

(2) W 为一群, 且 $W=\langle S\rangle$;

(3) $R=\{(s_is_j)^{m_{ij}}=1 \mid i,j\in I\}$ 为 W 关于生成元集 S 的定义关系.

这时 (W,S) 也说是 I 上 Coxeter 系, W 叫做关于 M 的 Coxeter 群.

定义 2.4 设 (W,S) 为 Coxeter 系. 对于任意的 $w\in W$, w 的最短 (即包含生成元因子个数最少的) 表达式 $w=s_1s_2\cdots s_q$ 中因子 $s_i\in S$ 的个数 q 叫做 w 的长度 (length), 记作 $l(w)=q$.

定理 2.5 令 W 为一群, S 为 W 中某些二阶元之集合, 且 $W=\langle S\rangle$. 则 (W,S) 为一 Coxeter 系, 当且仅当如下的交换性条件成立: 设 $w=s_1\cdots s_q\in W, s_i\in S, l(w)=q$. 则对于 $s\in S$, 只要 $l(sw)\le l(w)=q$, 便可找到 $j, 1\le j\le q$, 使以下等式成立: $ss_1\cdots s_{j-1}=s_1\cdots s_j$.

为了证明定理 2.5 我们先证明如下的引理.

引理 2.6 设 (W,S) 为 I 上 Coxeter 系. 令

$$T=\{t\in W \mid \exists w\in W, t^w\in S\}.$$

对于序列 $\mathfrak{s}=(s_1,\cdots,s_q), s_i\in S$, 定义

$$N(\mathfrak{s},t)=\{i \mid t=s_i^{s_{i-1}\cdots s_1}, 1\le i\le q\}.$$

如果 $\mathfrak{s}=(s_1,\cdots,s_q)$, $\mathfrak{s}'=(s'_1,\cdots,s'_r)$, 而且 $s_1\cdots s_q=s'_1\cdots s'_r$, 则成立:

$$|N(\mathfrak{s},t)|\equiv|N(\mathfrak{s}',t)| \pmod 2,\ \forall t\in T.$$

证 记 $X=\{\pm1\}\times T$. 对于 $s\in S$, 定义 X 的置换 U_s 如下: 对于 $(\varepsilon,t)\in X$, 规定

$$(\varepsilon,t)^{U_s}=(\varepsilon\delta(s,t),t^s),$$

其中 $\delta(s,t)=-1$, 若 $s=t$; $\delta(s,t)=1$, 若 $s\neq t$. 显然 $U_s^2=1$. 以下证明映射 $s\mapsto U_s$ 可以扩充为群 W 到 $\mathrm{Sym}X$ 内的一个同态对应. 由 W 之定义可知, 我们仅需证明这一映射保持 W 的定义关系 R, 即证明

$$(U_{s_i}U_{s_j})^{m_{ij}}=1,\ \forall i,j\in I.$$

设 $s,\ s'\in S, o(ss')=m$, 则对于 $k<m$ 成立:

$$(\varepsilon,t)^{(U_sU_{s'})^k}=(\pm\varepsilon,(ss')^{-k}t(ss')^k).$$

注意, 由定义, 对于 $k+1$, ε 变号当且仅当

$$(ss')^{-k}t(ss')^k=s\text{或}ss's.$$

以上结果相当于 $t=(ss')^{2k}s$ 或 $t=(ss')^{2k+1}s$, 其中整数 k 遍历 0 到 $m-1$. 若 $t=(ss')^ls$, $l<m$, 则有 $t=(ss')^{l+m}s$, 这表明, 对于上述形状的 t, ε 的符号改变两次. 从而 $(U_sU_s')^m=1$, 即映射保持 W 的定义关系.

故对于 $w=s_1\cdots s_q\in W, s_i\in S$, 有

$$(\varepsilon,t)^{U_w}=(\varepsilon,t)^{(U_{s_1}\cdots U_{s_q})}=(\varepsilon(\prod_{i=1}^{m}\delta(s_i,t^{s_1\cdots s_{i-1}})),t^w),$$

其中 $\delta(s_i,t^{s_1\cdots s_{i-1}})=-1$ 当且仅当 $i\in N(\mathfrak{s},t)$. 故 $(\varepsilon,t)^{U_w}=((-1)^{|N(\mathfrak{s},t)|},t^w)$. 这就证明了, $|N(\mathfrak{s},t)|(\mathrm{mod}\ 2)$ 仅依赖于 w 而与 $\mathfrak{s}$ 的选择无关. □

引理 2.7 令 (W,S) 为一 Coxeter 系, $w=s_1\cdots s_q\in W$. 令 $\mathfrak{s}=(s_1,\cdots,s_q)$, 并规定

$$\eta(\mathfrak{s})=|\{t\in T\mid N(\mathfrak{s},t)\equiv1(\mathrm{mod}\ 2)\}|.$$

则有 $\eta(\mathfrak{s})=l(w)$.

证 由引理 2.6 可知，若 $\mathfrak{s}'=(s_1',\cdots,s_r')$ 能使 $w=s_1'\cdots s_r'$，则 $\eta(\mathfrak{s})=\eta(\mathfrak{s}')$.

不失一般性，可假定 $l(w)=q$. 显然 $\eta(\mathfrak{s})\le l(w)=q$. 若 $\eta(\mathfrak{s})<q$, 则有 i,j, $1\le i<j\le m$, 能使 $s_i^{s_{i-1}\cdots s_1}=s_j^{s_{j-1}\cdots s_1}$, 故有 $s_is_{i+1}\cdots s_{j-1}=s_{i+1}\cdots s_j$, 从而有

$$w=s_1\cdots s_{i-1}s_i\cdots s_{j-1}s_j\cdots s_q=s_1\cdots s_{i-1}s_{i+1}\cdots s_{j-1}s_{j+1}s_q.$$

则 $l(w)=q-2$, 这与 $\mathfrak{s}$ 之选择相矛盾. □

定理 2.5 之证明:

必要性: 假定 (W,S) 为一 Coxeter 系. 令 $s=s_0$, 则 $l(s_0w)=l(s_0s_1\cdots s_q)\le l(w)=q<q+1$. 则由引理 2.7 可知，存在 $i<j$ 能使

$$s_is_{i+1}\cdots s_{j-1}=s_{i+1}\cdots s_j, 1\le i<j\le q.$$

若 $i>0$, 则重复引理 2.7 之证明过程便可得出 $l(w)<q$, 矛盾. 故仅可能有 $i=0$, 而这正表明，交换性条件成立.

充分性: 设 W 为一群，S 为 W 中某些 2 阶元之集合，且对于 (W,S), 交换性条件成立. 我们证明 (W,S) 为一 Coxeter 系. 为此，证若 α 为 S 到任意群 G 内的映射，且 α 保持关系 R, 则 α 可扩充为 W 到 G 的同态.

首先，我们定义 W 到 G 内的一个映射 $\tilde{\alpha}$. 令 $w=s_1\cdots s_q=s_1'\cdots s_q'\in W$, 其中 $s_i,s_i'\in S, l(w)=q$.

我们证明

$$s_1^\alpha\cdots s_q^\alpha=s_1'^\alpha\cdots s_q'^\alpha.$$

假定 w 为一具有极小长度的反例. 显然 $l(s_1'w)\le q-1<q$. 则由交换性条件可知有 $j\le q$ 能使

$$s_1's_1\cdots s_{j-1}=s_1\cdots s_j.$$

若 $j<q$, 则有 $w=s_1's_1\cdots s_{j-1}s_{j+1}\cdots s_q=s_1'\cdots s_q'$, 即有

$$s_1\cdots s_{j-1}s_{j+1}\cdots s_q=s_2'\cdots s_q'.$$

由 q 的极小性，便得

$$s_1^\alpha\cdots s_{j-1}^\alpha s_{j+1}^\alpha\cdots s_q^\alpha=s_2'^\alpha\cdots s_q'^\alpha. \tag{2.1}$$

这样就有

$$s_1'^\alpha s_1^\alpha\cdots s_{j-1}^\alpha=s_1^\alpha\cdots s_j^\alpha. \tag{2.2}$$

将 (2.2) 代入 (2.1), 便得 $s_1^\alpha\cdots s_q^\alpha=s_1'^\alpha\cdots s_q'^\alpha$, 与 w 为反例的假定矛盾.

故仅需考虑情况 $j=q$. 我们分别以 $\{s_1',s_1,\cdots,s_{q-1}\}$ 和 $\{s_1,s_1',\cdots,s_{q-1}'\}$ 代替 $\{s_1,\cdots,s_q\}$ 和 $\{s_1',\cdots,s_q'\}$, 并且重复以上讨论，最终可以得到如下关系式：

$$(s's)^{q/2}=(ss')^{q/2}, \text{若 } q \text{为偶},$$

或

$$s(s's)^{(q-1)/2}=s'(ss')^{q-1/2}, \text{若 } q \text{ 为奇}.$$

注意上两式中 $\{s,s'\}=\{s_1,s_1'\}$, 但相应于 (2.1) 式的关系却不能成立. 由以上两式可得 $(ss')^q=1$, 从而 $o(ss')\mid q$. 由假设， α 保持 R 不变，故 $o(s^\alpha s'^\alpha)\mid q$, 从而 $(s^\alpha s'^\alpha)^q=1$, 由此立得矛盾.

至此, 我们可定义 $\tilde\alpha: W\longrightarrow G$ 如下: 若 $w=s_1\cdots s_q, l(w)=q$, 定义 $w^{\tilde\alpha}=s_1^\alpha\cdots s_q^\alpha$. 以上讨论表明，这样的 $\tilde\alpha$ 是唯一确定的.

下面我们证明 $\tilde\alpha$ 为 W 到 G 内的同态. 我们先证明 $(sw)^{\tilde\alpha}=s^\alpha w^{\tilde\alpha}$. 若 $l(sw)=q+1$, 结论显然成立. 若 $l(sw)\le q$, 则由交换性条件, 有 $j\le q$, 能使 $ss_1\cdots s_{j-1}=s_1\cdots s_j$. 易知, 这时 $l(s_1\cdots s_j)=j$, 故有 $s^\alpha s_1^\alpha\cdots s_{j-1}^\alpha=s_1^\alpha\cdots s_j^\alpha$. 由于 $sw=s_1\cdots s_{j-1}s_{j+1}\cdots s_q$, 故 $l(sw)\le q-1$. 又由于 $l(w)=q$, 故 $l(sw)=q-1$, 从而由 $\tilde\alpha$ 之定义有

$$(sw)^{\tilde\alpha}=s_1^\alpha\cdots s_{j-1}^\alpha s_{j+1}^\alpha\cdots s_q^\alpha=s^\alpha s_1^\alpha\cdots s_j^\alpha s_{j+1}^\alpha\cdots s_q^\alpha=s^\alpha w^{\tilde\alpha}.$$

下面我们证明 $(w'w)^{\tilde\alpha}=w'^{\tilde\alpha}w^{\tilde\alpha}$.

我们对 $l(w')$ 进行归纳. 令 $w'=s'w_1'$, 其中 $l(w_1')=l(w')-1, s'\in S$, 则由以上讨论得：

$$(w'w)^{\tilde\alpha}=(s'w_1'w)^{\tilde\alpha}=s'^{\tilde\alpha}(w_1'w)^{\tilde\alpha}=s'^\alpha w'^{\tilde\alpha}w^{\tilde\alpha}=w'^{\tilde\alpha}w^{\tilde\alpha}.$$

这就证明了 (W,S) 为一 Coxeter 系. □

定理 2.8 设 (W,S) 为一 Coxeter 系. 则

(1) 若 $w=s_1\cdots s_q, s_i\in S, l(w)=q$, 则集合 $\{s_1,\cdots,s_q\}$ 由 w 所唯一确定;

(2) 设 $J\subseteq S$, $W_J=\langle J\rangle$. 若 $w\in W_J$ 且 $w=s_1\cdots s_q$ 为 w 的最短表达式, 则所有的因子 $s_i\in J$;

(3) 依 (2) 中记法, (W_J,J) 为一 Coxeter 系.

证 (1) 定义

$$D_w=\{\mathfrak{s}=(s_1,\cdots,s_q)\,\big|\,w=s_1\cdots s_q, s_i\in S\}.$$

对任意 $\mathfrak{s}=(s_1,\cdots,s_q)\in D_w$, 规定 $f(\mathfrak{s})=\{s_1,\cdots,s_q\}\subseteq S$. 则我们可仿照定理 2.5 之证明过程, 完成 (1) 的证明. (作为练习, 请读者自行写出证明细节.)

(2) 设由 (1) 中 $f(\mathfrak{s})$ 所确定之集合为 S_w, 则 S_w 为 S 的子集, 且成立 $S_{w^{-1}}=S_w$, $S_{sw}\subseteq\{s\}\cup S_w$, 从而 $S_{uw}\subseteq S_u\cup S_w$, 其中 $u,w\in W$. 故集合 $W_1=\{w\,\big|\,S_w\subseteq J\}$ 为 W 的一个子群. 由 $s\in J$ 可得 $S_s\subseteq J$. 故有 $s\in W_1$, 从而 $J\subseteq W_1$, 特别地 $W_J\leq W_1$. 但对 W_1 中任意元 w, 总有 $S_w\subseteq J$, 故 $W_1=W_J$. 即 (2) 成立.

(3) 令 $w\in W_J$, w 在 (W_J,J) 中的长度与 w 在 (W,S) 中的长度相同, 故对 (W,S) 交换性条件成立保证了对 (W_J,J) 交换性条件也成立. 从而 (W_J,J) 为一 Coxeter 系. □

设 $M=(M_{ij}), i,j\in I$ 为 I 上 Coxeter 矩阵, I 可分解为二个无交非空集 I' 和 I'' 的并, 且能使 $m_{i'i''}=2, \forall i'\in I', i''\in I''$. 则 $M'=(m_{ij}), i,j\in I'$ 和 $M''=(m_{ij}), i,j\in I''$ 均为 Coxeter 矩阵, 且 M 的 D-图为 M' 的 D-图与 M'' 的 D-图的并. 这时我们说 M 是 M' 与 M'' 之直和. 一个非空并且不能表为直和的 D-图称为不可分的.

命题 2.9 令 (W,S) 为一 Coxeter 系, Γ 为相应的 D-图. 若 Γ 非连通, 则 S 可表为两个不相交子集 S_1 和 S_2 的并. 令 $W_i=$

$\langle S_i\rangle$, $i=1,2$, 则 (W_i,S_i) 为 Coxeter 系 $(i=1,2)$, 并有直积分解 $W\cong W_1\times W_2$. 反之, 若 W 为 W_1 和 W_2 之直积, 则相应的 D-图 Γ 为非连通的.

证 可设 Γ 之顶点等同于集合 S. 由假定, Γ 为非连通的, 设 S_1 为一个连通成分之顶点集合, 并令 $S_2=S\backslash S_1$. 则 S_1 和 S_2 为 S 中两个非空且不相交的子集. 对于 $s\in S_1, t\in S_2$, 顶点 s 和 t 在 Σ 中是不相连的, 这表明 $o(st)=2$, 即 s, t 可换. 这样就证明了 W_1 和 W_2 元素可换. 设 $w\in W_1\cap W_2$, 则由定理 2.8(2), w 的最短表达式可写作 $S_1\cap S_2$ 中元素之积. 但 $S_1\cap S_2=\varnothing$, 故 $W_1\cap W_2=1$. 从而 $W\cong W_1\times W_2$. 由定理 2.8(3) 可知, (W_i,S_i) 为一 Coxeter 系. 逆命题显然成立. □

定义 2.10 Coxeter 系 (W,S) 说是不可约的, 若与之相应的 D-图是连通的.

定义 2.11 设 Σ 为一薄室复形, Σ 上一个态射 φ 说是一个迭合 (folding), 若 φ 是幂等的且 $\forall C\in(\text{Cham }\Sigma)^{\varphi}$, C 是 Σ 中两个室 C 和 C' 在 φ 之下的象. Σ 在迭合 φ 之下的像说是一个根 (root), Σ 说是一个 Coxeter复形, 若对 Σ 中任一对相邻的室 C' 和 C, 都有 Σ 的迭合, 把 C' 映到 C.

命题 2.12 令 Σ 为一 Coxeter 复形. 假定 Σ 中两个室 C 和 C' 相邻, 则在 Σ 中有迭合 φ 和 φ' 能使 $C'^{\varphi}=C$ 且 $C^{\varphi'}=C'$. φ 和 φ' 是 Σ 上仅有的满足上述条件的迭合. 且成立

$$\Sigma=\Sigma^{\varphi}\cup\Sigma^{\varphi'},\text{Cham }(\Sigma^{\varphi})\cap\text{Cham }(\Sigma^{\varphi'})=\varnothing.$$

如下定义的映射 σ:

$$A^{\sigma}=\begin{cases}A^{\varphi'},\text{若}A\in\Sigma^{\varphi};\\ A^{\varphi},\text{若}A\in\Sigma^{\varphi'}.\end{cases}$$

为 Σ 的一个 2 阶自同构, 叫做 Σ 的关于室 C 和 C' 的反射 (reflection)(或叫做关于 C 中墙 $C\cap C'$ 的反射, 或简称为关于 C 的一个反射).

证　注意由迭合的幂等性可知, $\forall A \in \Sigma^{\varphi}$, 总成立 $A^{\varphi} = A$. 设 D 为 Σ 中任意室, 假定 $\mathrm{dist}\, BD = m$, 此处 $B = C \cap C'$. 令 $\mathbf{G} = (C_0, C_1, \cdots, C_m = D)$ 为连接 B 和 D 的最短廊. 我们先证明如下的性质 (*).

(*)　若 $D \in \Sigma^{\varphi}$, 则 $C_0 = C$, 这时 $C_i \in \Sigma^{\varphi}$, $\forall 1 \leq i \leq m-1$; 而若 $D \notin \Sigma^{\varphi}$, 则 $C_0 = C'$.

假定 $D \in \Sigma^{\varphi}$, 但 $C_0 = C'$, 则有 $i : 0 \leq i \leq m-1$, 能使 $C_{i+1} \in \Sigma^{\varphi}$, $C_i \notin \Sigma^{\varphi}$. 由迭合之定义 $C_i^{\varphi} \neq C_i$. 由于 $C_{i+1}^{\varphi} = C_{i+1}$, 故 $(C_i \cap C_{i+1})^{\varphi} = C_i \cap C_{i+1}$. 这表明 C_i^{φ} 包含 $C_i \cap C_{i+1}$. 由于 $C_i \cap C_{i+1}$ 为一墙, 且 Σ 为薄, 故 C_i 和 C_{i+1} 为 Σ 中仅有的包含 $C_i \cap C_{i+1}$ 的室, 这就迫使 $C_i^{\varphi} = C_{i+1}$, 从而 $\mathbf{G}^{\varphi}$ 为连接 B, D 的廊, 且萎缩, 矛盾. 这就证明了 $C = C_0$. 同法可证 $C_i \in \Sigma^{\varphi}$.

现假定 $D \notin \Sigma^{\varphi}$, 且 $C_0 = C$. 这时有 i, $0 \leq i < m$ 能使 $C_i \in \Sigma^{\varphi}$, $C_{i+1} \notin \Sigma^{\varphi}$, 且 i 为极小. 对于 $C_j, 0 \leq j \leq i$, 令 $C_j' \neq C_j$, $(C_j')^{\varphi} = C_j$. 我们断言: $\forall j < i$, C_j' 与 C_{j+1}' 相邻接, 而 $C_i' = C_{i+1}$. 以 U 表示 $C_j \cap C_{j+1}$ 在 φ 之下的原像. E 表示包含 U 且不等于 C_j' 的室. 则 $E^{\varphi} = C_j$ 或 C_{j+1}. 以下我们分别考虑两种情况: (i) $E^{\varphi} = C_j$. 由迭合之定义, 必有 $E = C_j$. 这时 $U = U^{\varphi}$, 故有 $C_j' = C_{j+1}$, 从而 $j = i$. (ii)$E^{\varphi} = C_{j+1}$. 这时 $E = C_{j+1}'$, 故 C_j' 与 C_{j+1}' 相邻接.

由以上讨论可知, 存在连接 BD 且长不超过 $m-1$ 的廊 $\widetilde{\mathbf{G}} = (C_0' = C', C_1', \cdots, C_i' = C_{i+1}, C_{i+2}, \cdots, D)$, 与假定 $\mathrm{dist}\, BD = m$ 相矛盾.

由 (*) 立知 $\mathrm{Cham}\,(\Sigma^{\varphi}) \cap \mathrm{Cham}\,(\Sigma^{\varphi'}) = \varnothing$ 且 $\mathrm{Cham}\,(\Sigma) = \mathrm{Cham}\,(\Sigma^{\varphi}) \cup \mathrm{Cham}\,(\Sigma^{\varphi'})$, 由第二个结论立得 $\Sigma = \Sigma^{\varphi} \cup \Sigma^{\varphi'}$.

若 $D \in \mathrm{Cham}\,(\Sigma^{\varphi'})$, 则对 m 归纳即可证明 $D^{\varphi\varphi'} = D$.

现在我们证明, 若 C 和 C' 相邻, 则满足条件 $C'^{\varphi} = C$ 的迭合 φ 是唯一的. 为此仅需证: 若 ψ 也是 Σ 的一个迭合, 且使 $C'^{\psi} = C$, 则 $D^{\varphi} = D^{\psi}$, $\forall D \in \mathrm{Cham}\,(\Sigma)$. 我们用归纳法证明所需结论. 若 $m = 0$, 结论显然成立, 故以下假定 $m > 0$.

若 $D \in \Sigma^{\varphi}$, 则 $C_0 = C$ 且 $C_i \in \Sigma^{\varphi}$, 这时必然有 $D \in \Sigma^{\psi}$, 否则将有 $C_0 = C'$. 从而在 D 的一切面上 ψ 与 φ 作用相同.

现假定 $D \in \Sigma^{\varphi'}$, 则必然有 $D \in \Sigma^{\psi'}$ 且

$$C_i \in \Sigma^{\varphi'}, C_i \in \Sigma^{\psi'}, i = 0, 1, 2, \cdots, m.$$

由于 $(\mathbf{G}^{\varphi})^{\varphi'} = \mathbf{G}$, 故 $C_i^{\varphi} \neq C_j^{\varphi}, \forall i \neq j$. 由归纳假定

$$(C_{m-1} \cap D)^{\varphi} = (C_{m-1} \cap D)^{\psi},$$

而 C_{m-1}^{φ} 与 D^{φ} 为 Σ 中仅有的包含墙 $C_{m-1} \cap D$ 的室, 又 C_{m-1}^{ψ} 与 D^{ψ} 也为包含墙 $C_{m-1} \cap D$ 的室, 且 $C_{m-1}^{\varphi} = C_{m-1}^{\psi}$, 故 $D^{\varphi} = D^{\psi}$, 从而对于 $P = D \backslash (C_{m-1} \cap D)$ 成立 $P^{\varphi} = P^{\psi}$, 故 φ 和 ψ 对于 D 的一切面作用相同, 这就证明了 $\varphi = \psi$.

令 σ 为 Σ 的自态射, 且成立:

$$A^{\sigma} = \begin{cases} A^{\varphi'}, \text{若} A \in \Sigma^{\varphi}; \\ A^{\varphi}, \text{若} A \in \Sigma^{\varphi'}. \end{cases}$$

因对任意 $A \in \Sigma^{\varphi} \cap \Sigma^{\varphi'}$, 成立 $A^{\varphi} = A = A^{\varphi'}$, 故 σ 是唯一确定的. 对于 $A \in \Sigma^{\varphi}$ 成立 $A = (A^{\varphi'})^{\varphi}$. 同样对于 $A \in \Sigma^{\varphi'}$, 成立 $A = (A^{\varphi})^{\varphi'}$. 这表明 σ^2 为恒等元. 由 σ 之定义可知, σ 为 Σ 上 1-1 态射, 即 σ 为 Σ 的 2 阶自同构. □

定义 2.13 由 Coxeter 复形 Σ 中全体反射所生成的 Σ 的自同构群叫做 Σ 的 Weyl群, 记作 $W(\Sigma)$.

定理 2.14 令 Σ 为 Coxeter 复形, W 为 Σ 的 Weyl 群. 令 C 为 Σ 的一个室, S 为关于 C 的全体反射之集合, 则成立:

(1) $W = \langle S \rangle$;

(2) W 为 Σ 的全自同构群;

(3) W 在 Σ 的室之集合上正则 (关于置换群的正则的概念, 参见第 XII 章定义 1.10).

证　令 $W_1 = \langle S \rangle$, W_2 为 Σ 的全自同构群. 显然 $W_1 \le W \le W_2$.

首先证明 W_1 在 Σ 的全体室集合上传递. 令 D 为 Σ 中一室, $m = \text{dist } CD$, 则有长为 m 的廊 $\mathbf{G} = (C_0 = C, C_1, \cdots, C_m = D)$. 对 m 施行归纳, 证明存在 $w \in W_1$, 使 $C^w = D$.

若 $m = 0$, 只需令 $w = 1$ 即可. 设 $m > 0, B = C \cap C_1$. 则有关于墙 B 的反射 $\sigma \in S$ 能使 $C_1^\sigma = C, C_2^\sigma, \cdots, C_m^\sigma = D^\sigma$ 为一长为 $m-1$ 的廊. 由归纳假定, 可找到 $w_1 \in W_1$, 使 $C^{w_1} = D^\sigma$. 令 $w = w_1\sigma$. 则有 $C^w = C^{w_1\sigma} = D$. 这就证明了群 W_1 在 Σ 的室集合上传递.

以下证明 W_2 在 Σ 的室集合上是正则的. 假定对于 $w, w' \in W_2$ 成立 $C^w = C^{w'}$. 令 $w'' = w'w^{-1}$, 则 $C^{w''} = C$. 对每个特定的型, 室 C 中恰包含一个具有该型的面, 故 w'' 固定 C 中每一个面. 又因为 Σ 是薄的, 故 w'' 固定每一个与 C 相邻的室及其中一切面. 通过归纳可证明 w'' 为恒等元, 故 $w = w'$. 这表明 W 在室集合上正则.

现在我们可以很容易地得出所有结论. 令 $w_2 \in W_2$, 则 C^{w_2} 为一室. 因 W_1 在 Σ 的室集合上传递作用, 则有 $w_1 \in W_1$ 能使 $C^{w_1} = C^{w_2}$. 因 W_2 在 Σ 上正则, 且 $W_1 \le W_2$, 故 $w_2 = w_1 \in W_1$. 从而得 $W_1 = W = W_2$. 这样就证明了 (1), (2), (3) 成立.　□

现在我们考察 Coxeter 复形 Σ 的 Weyl 群 $W(\Sigma)$. 我们证明 $W(\Sigma)$ 为一 Coxeter 群, 并讨论与 $W(\Sigma)$ 有关的一些性质.

定理 2.15 令 Σ 为一 Coxeter 复形, W 为 Σ 的 Weyl 群. 令 C 为 Σ 中一个固定的室, S 为关于 C 的所有墙的反射之集合.

(1) 令 $w_1, w_2 \in W$, 则 C^{w_1} 与 C^{w_2} 为相邻的室当且仅当 $\exists s \in S$ 使 $w_1 = sw_2$;

(2) 若 $(C^{w_0}, C^{w_1}, \cdots, C^{w_k})$ 为一廊, 其中任二项不同, 则有 S 中元素序列 $s_1, \cdots, s_k$ 能使 $w_k = s_k s_{k-1} \cdots s_1 w_0$. 特别地 $l(w_k w_0^{-1}) \le k$;

(3) $\forall w \in W$, 成立 $\text{dist } CC^w = l(w)$.

证 (1) 若 C^{w_1} 和 C^{w_2} 为相邻的, 则 C 和 $C^{w_1w_2^{-1}} = (C^{w_1})^{w_2^{-1}}$ 有一公共墙 B. 令 s 为关于 B 的反射, 则有 $C^s = C^{w_1w_2^{-1}}$. 由于 Σ 的 Weyl 群在 Σ 上是正则的, 故有 $s = w_1w_2^{-1}$, 即 $w_1 = sw_2$. 反之, 若 $w_1 = sw_2$, 则 C^{w_2} 与 $C^{sw_2} = C^{w_1}$ 有一公共墙, 故 C^{w_1} 与 C^w 相邻.

(2) 由廊的定义, C^{w_i} 与 $C^{w_{i+1}}$ 相邻. 则由 (1), 可找到 $s_{i+1} \in S$, 使 $w_{i+1} = s_{i+1}w_i$. 故有 $w_k = s_ks_{k-1}\cdots w_0$. 又由长度之定义, 立得 $l(w_kw_0^{-1}) \le k$.

(3) 由 (2) 成立 $l(w) \le \text{dist}\ CC^w$. 令 $w = s_1\cdots s_q, l(w) = q$, 便有长为 q 的廊连接 C 和 C^w. 故 $\text{dist}\ CC^w \le q$. 这表明 $l(w) = \text{dist}\ CC^w$. □

定理 2.16 *令 W 为 Coxter 复形 Σ 的 Weyl 群. 若 S 为关于 Σ 中某一确定的室的全体反射之集合, 则 (W, S) 为一 Coxeter 系.*

证 由定理 2.5 及 S 之定义, 我们只需证明交换性条件成立. 假定 $w = s_1\cdots s_q, s_i \in S$ 为 w 的最短表达式, 且 $l(sw) \le q$, 对于某个 $s \in S$ 成立. 由定理 2.15, $(C, C^{s_1}, \cdots, C^{s_qs_{q-1}\cdots s_1})$ 为连接 C 和 $C^{w^{-1}}$ 的最短廊.

由假定, $l(sw) \le q$, 故 C 和 C^{sw} 之距离不超过 q. 从而有 $\text{dist}\ C^sC^{w^{-1}} \le q$. C 与 C^s 相邻, 可设 B 为二者之公共墙. 令 φ 为把 C^s 变到 C 的迭合, 则对一切不包含在 Σ^φ 内的室, φ 与 s 作用相同.

假定 $C^{w^{-1}} \in \Sigma^\varphi$. 由于 $\text{dist}\ C^sC^{w^{-1}} \le q$, 故有长度不超过 q 的廊 $\mathbf{G}$ 连接 C^s 和 $C^{w^{-1}}$, 从而 $\mathbf{G}^\varphi$ 为连接 C 和 $C^{w^{-1}}$ 的廊. 由于 $C^s \notin \Sigma^\varphi$, 故 $\mathbf{G}$ 包含相邻的室 D 和 D', 能使 $D \notin \Sigma^\varphi$, $D' \in \Sigma^\varphi$. 则 $D^\varphi = D'$, 从而 $\mathbf{G}^\varphi$ 萎缩, 这与 $\text{dist}\ CC^{w^{-1}} = q$ 相矛盾. 因此 $C^{w^{-1}} \notin \Sigma^\varphi$. 故关于廊 $(C, C^{s_1}, \cdots, C^{w^{-1}})$, 必可找到整数 j, 使

$$C^{s_{j-1}\cdots s_1} \in \Sigma^\varphi.$$

而

$$C^{s_js_{j-1}\cdots s_1} \notin \Sigma^\varphi.$$

故有

$$C^{s_{j-1}\cdots s_1}=(C^{s_j\cdots s_1})^{\varphi}=C^{(s_j\cdots s_1)s}.$$

由 Weyl 群作用的正则性，故有

$$ss_1\cdots s_{j-1}=s_1\cdots s_j.$$

这表明，对于 (W,S)，交换性条件成立．故 (W,S) 为一 Coxeter 系．□

定理 2.14 的逆也成立，我们有如下定理：

定理 2.17 令 (W,T) 为一 Coxeter 系，$T=\{t_i \mid i\in I\}, W_i=\langle t_j \mid i\neq j\rangle$．令 $\Sigma=\{W_ix \mid i\in I\}$．$W$ 通过右乘作用在陪集集合 Σ 上．若把 Σ 看做关于子群集 $\{W_i \mid i\in I\}$ 的陪集复形，则 Σ 为一 Coxeter 复形，W 为 Σ 的 Weyl 群，T 为关于室 $C=\{W_i \mid i\in I\}$ 的所有墙的反射之集合．

这一定理的证明留给读者．(见习题 3)

定理 2.18 设 Σ 为一 Coxeter 复形，A 为 Σ 中具有型 $I\backslash\{i,j\}$ 的面，C,D 为 st A 中任意室，则 dist $CD\leq m_{ij}$，且有室 $E\in$ st A，能使 dist $CE=m_{ij}$．st A 中室的总数为 $2m_{ij}$，即 Σ 恰有 $2m_{ij}$ 个包含 A 的室．

证　首先我们证明，若室 $D\in$ st A，$\mathbf{G}$ 为连接 C 和 D 的最短廊：$\mathbf{G}=(C_0=C,C_1,\cdots,C_k=D)$，则对任意 $i\in\{0,1,\cdots,k\}$，成立 $C_i\in$ st A．我们对 k 进行归纳．若 $k=1$，显然成立．设 $k>1$．对于墙 $B=C\cap C_1$，有关于 B 的迭合 φ,φ'，使得 $C^{\varphi}=C_1, C_1^{\varphi'}=C$．假定 $A\not\subset C_1$，则 $A^{\varphi}\neq A$．从而 $D\notin\Sigma^{\varphi}$，故 $D\in\Sigma^{\varphi'}$，

$$\mathbf{G}^{\varphi'}=(C_1^{\varphi'}=C,C_2^{\varphi'},\cdots,C_{k-1}^{\varphi'},D)$$

为连接 C 和 D 的最短廊，与 $\mathbf{G}$ 为最短廊之假定矛盾．这意味着必有 $A\subset C_1$．这时 $\mathbf{G}_1=(C_1,\cdots,D)$ 为连接 C 和 D 的最短廊，

$C_1, D \in \text{st } A$, $\mathbf{G}_1$ 的长度为 $k-1$. 由归纳假定, $\mathbf{G}_1$ 中每个室都属于 st A, 这就证明了我们的论断.

设 $D \in \text{st } A$, 则有 w 能使 $D = C^w$. 令 $\mathbf{G}$ 为如上所定义连接 C 和 D 的最短廊, 其中 $C_i \in \text{st } A$, $\forall i \in \{0, 1, \cdots, k\}$. 由于 C_i 与 C_{i+1} 相邻, 故有 $s \in S$, 能使 $C_{i+1} = C_i^s$. 但 s 作为自同构是保型的, 故 $s = s_i$ 或 s_j. 这就证明了 $w = s_i s_j s_i \cdots$ 或$s_j s_i s_j \cdots$. 又由于 $(s_i s_j)^{m_{ij}} = 1$, 故对任意的 $w = s_i s_j s_i \cdots$ 或$s_j s_i s_j \cdots$, 都成立 $l(w) \leq m_{ij}$. 又我们总可以找到 $w = s_i s_j s_i \cdots$ 或$s_j s_i s_j \cdots$, 使得 $l(w) = m_{ij}$. 对这样的 w, 由定理 2.15(3), 成立 dist $CC^w = m_{ij}$. 又易知: $C, C^{s_i}, C^{s_j}, C^{s_i s_j}, C^{s_j s_i}, \cdots, C^{\overbrace{s_i s_j s_i \cdots}^{m_{ij}\text{个因子}}}$ 均不相同. 且其中除 1 和 $\overbrace{s_i s_j s_i \cdots}^{m_{ij}\text{个因子}}$ 外, 具有相同长度的 $s_i s_j s_i \cdots$ 和 $s_j s_i s_j \cdots$ 成对出现. 这就证明了, 包含 A 的室恰有 $2m_{ij}$ 个. □

有限不可约 Coxeter 系可以进行完全分类, 下面我们简单介绍分类的基本思想.

令 (W, S) 为一秩为 n 的不可约 Coxeter 系, 其中 $S = \{s_1, \cdots, s_n\}$, 定义关系 $R = \{(s_i s_j)^{m_{ij}} = 1 \mid i, j \in I\}$. 令 V 为实数域 $\mathbb{R}$ 上 n 维向量空间, $\{u_1, \cdots, u_n\}$ 为 V 的一组基. 定义双线性型 B 如下:

$$B(u_i, u_j) = -\cos(\pi/m_{ij}), \ (i, j = 1, 2, \cdots, n).$$

显然 B 是对称的. 令 Q 为与 B 相连带的二次型, 则 $Q(v) = B(v, v)$, $\forall v \in V$. 这时 (V, Q) 为实数域 $\mathbb{R}$ 上正交空间.

我们还定义 V 上线性变换如下:

$$v^{\sigma_i} = v - 2B(u_i, v)u_i, (i = 1, 2, \cdots, n).$$

易知, W 为正交空间 (V, Q) 上的等矩群.

可以证明, 若 (W, S) 不可约且有限, 则以上定义的 (V, Q) 等距于一个 n 维欧氏空间.

最终我们有如下的分类定理:

定理 2.19 (W, S) 为有限不可约 Coxeter 系当且仅当它的 D-图具有上页图 2.1 所示的型.

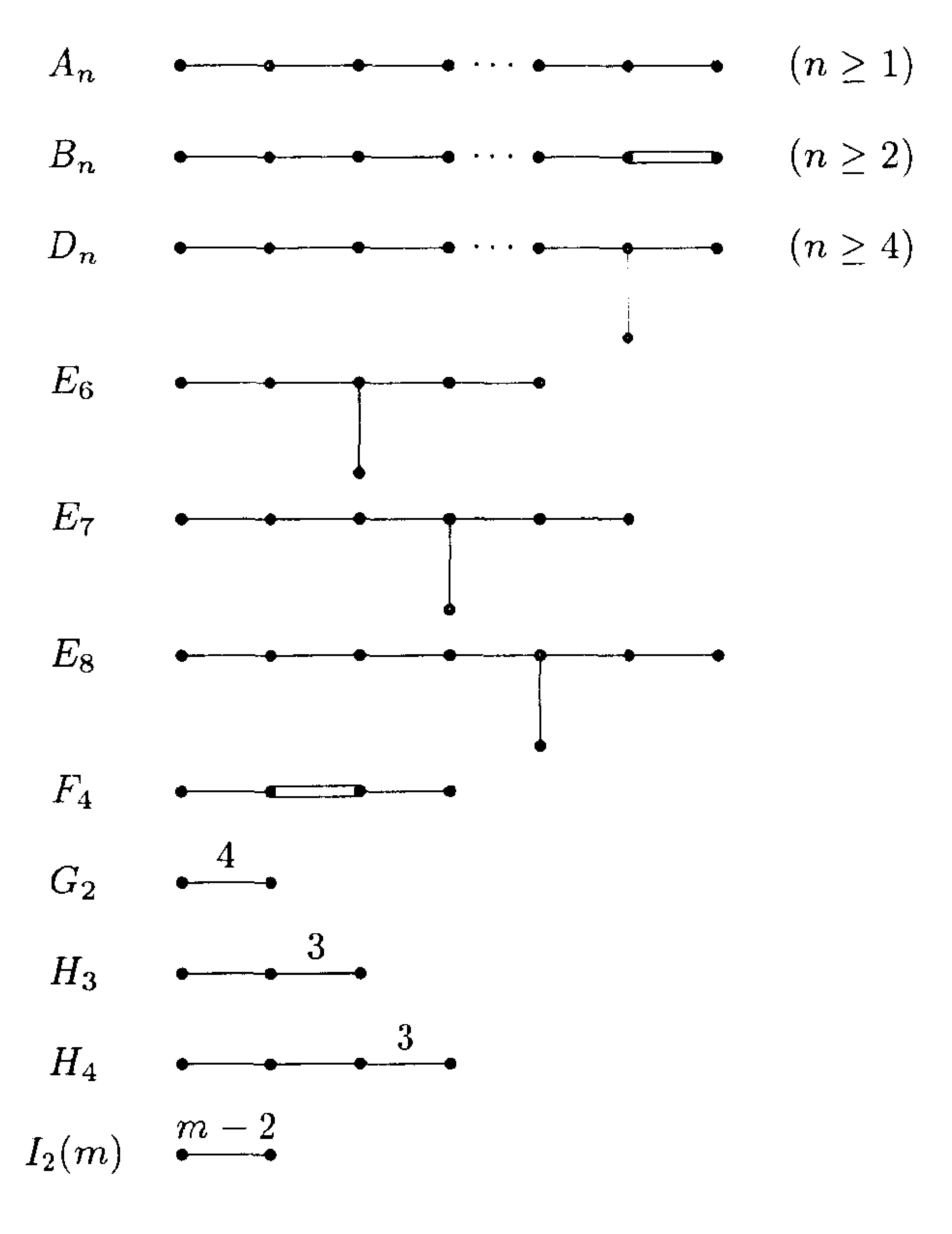


图 2.1

Coexeter 系的分类对于 Tits 几何理论和有限单群理论都具有十分重要的作用. 在以下的 §3 和 §4 中, 我们将对此有进一步的说明.

§3. 厦

本节给出了厦和寓的概念, 介绍了厦的一些性质. 讨论了厦与 Coxeter 复形及其 D-图的关系.

定义 3.1 令 Δ 为一室复形, $\mathcal{A}$ 为 Δ 的某些子复形之集合, 则序对 $(\Delta, \mathcal{A})$ 叫做一个厦, $\mathcal{A}$ 的元叫做 寓(apartment), 若下列条

件成立:

(B1) Δ 为厚的;

(B2) $\mathcal{A}$ 中的元为秩 d 薄室复形;

(B3) $\forall A, B \in \Delta$, 可找到 $\mathcal{A}$ 中一个元同时包含 A 和 B;

(B4) 若寓 Σ 和 Σ' 均同时包含 A 和 A', 则有 Σ 到 Σ' 的同构 α 能使 A, A' 连同其一切面在 α 之下不变.

若对于 Δ, 仅 (B2)-(B4) 成立, 便叫做弱厦 (weak building).

(注意自八十年代中期以来, 满足定义 3.1 中 (B2)-(B4) 的复形都叫做厦.)

由 (B4) 可知, 一个厦 Δ 中所有的寓构成 Δ 中一个子复形同构类. Δ 中的寓也叫做 Δ 的 Weyl 复形.

由习题 5, 我们可以看到, 例 1.7 中所定义的 $\Delta(\mathcal{P})$ 是一个厦.

命题 3.2 设 C 为厦 Δ 中一个室, Σ 为包含 C 的寓. 则有唯一的 Δ 到 Σ 上的态射 ρ 具有如下性质: ρ 保持 C 中一切面不动, 且成立

(1) 若 $A \in \Sigma$, 则 $A^\rho = A$;

(2) 若 $A \subset B$, 则 $A^\rho \subset B^\rho$;

(3) 若 B 为 Δ 的一个室, 则 B^ρ 也是一个室. 一般地, $\mathrm{rk}\ B = \mathrm{rk}\ (B^\rho)$;

(4) 若室 B 与室 B' 相邻, 则 B^ρ 与 B'^ρ 相邻, 或者 $B^\rho = B'^\rho$;

(5) 若 $A^\rho \subset C$, 则成立 $A = A^\rho \subset C$.

证 对于任意 $A \in \Delta$, 由定义 3.1(B3), 可找到一个寓 Σ' 同时包含 C 和 A. 又由定义 3.1(B4), 有 Σ' 到 Σ 的同构 η', η' 固定包含于 C 中任意的面 B. 我们证明, $A^{\eta'}$ 与 Σ' 的选择无关. 令 Σ'' 也是包含 A 和 C 的一个寓, 则有 Σ'' 到 Σ 的同构对应 η'', 使 $B^{\eta''} = B, \forall B \subset C$. 我们只要能够证明 $A^{\eta'} = A^{\eta''}$, 则断言成立.

由 (B4) 有 Σ' 到 Σ'' 的同构 θ, 能使 $B^\theta = B$, 其中 B 为 C 中任意的面, 且 $A^\theta = A$. 从而 η' 和 $\theta \cdot \eta''$ 都是 Σ' 到 Σ 的同构对应, 且均使 C 的一切顶点不变动. 由于 Σ 为薄室复形, 故 $\eta'^{-1} \cdot \theta \cdot \eta''$

为 Σ 上恒等态射，从而有

$$\eta' = \theta \cdot \eta''.$$

显然成立：

$$A^{\eta'} = (A^{\theta})^{\eta''} = A^{\eta''}.$$

令 A^{ρ} 为诸 $A^{\eta'}$ 的共同值，我们便得到一个 Δ 到 Σ 的态射.

以下证明 (1)-(5) 成立.

(1) 若 $A \in \Sigma$, 则可令 $\Sigma' = \Sigma$, 并令 ρ 为 Σ 上恒等映射，则当然成立 $A^{\rho} = A$.

(2), (3) 可直接由同构定义得出 (实际上，由于 ρ 为态射，立知 (2), (3) 成立).

(4) $B \cap B'$ 为 B 和 B' 的公共墙，则 $(B \cap B')^{\rho}$ 也是 B^{ρ} 和 B'^{ρ} 的公共墙，由 (B3) 立知 (4) 成立.

(5) 由于 ρ 通过寓的同构而定义，这些同构均保持 C 中一切顶点不变，由态射定义可知，所有这些同构都是保型的，故 C 以外的顶点不可能映入 C, 因此 (5) 成立. □

命题 3.2 中所定义的映射 ρ, 叫做 Δ 到 Σ 上以 C 为中心的收缩 (retraction). 由命题 3.2(1) 可知， ρ 是幂等的. 对于固定的 Σ, C, ρ 通常记作 retr (Σ, C).

定理 3.3 *设 Σ 为厦 Δ 的一个寓， C 为 Σ 中一室且 $A \subset C$. 令 $\mathbf{G} = \{C_i\}$ 为连接 A 和 Δ 中某一室 D 的最短廊，则*

(1) 若 $D \in \Sigma$, 则所有的 $C_i \in \Sigma$.

(2) 若 $\rho = \text{retr}\,(\Sigma, C)$, 则 $\mathbf{G}^{\rho}$ 是连接 A 和 D^{ρ} 的最短廊，且 $\text{dist}\, AD = \text{dist}\, AD^{\rho}$.

证 (1) 令 $\mathbf{G}$ 为一长为 m 的廊. 因 $C_m = D \in \Sigma$, 故若 (1) 不成立，则必存在整数 $i < m$, 能使 $C_i \notin \Sigma$, $C_{i+1} \in \Sigma$. 由廊之定义，C_i 和 C_{i+1} 有公共墙 B. 因 Σ 为薄的，故 B 恰包含在 Σ 的两个室之中. 设 $E \neq C_{i+1}$ 为 Σ 中另一包含 B 的室. 令 $\sigma = \text{retr}\,(\Sigma, E)$, 则 $A^{\sigma} = A$ 且 $D^{\sigma} = D$. 故 $\mathbf{G}^{\sigma}$ 为一连接 A 和 D 的廊， C_i^{σ} 为 Σ

中包含 B 的室. 由于 $C_i^\sigma \neq E$, 则 $C_i^\sigma = C_{i+1} = C_{i+1}^\sigma$. 从而 $\mathbf{G}^\sigma$ 萎缩. 这与 $\mathbf{G}$ 为最短廊之假定相矛盾.

(2) 由 (B3), 有寓 Σ' 同时包含 C 和 D, 又由 (1), $\mathbf{G}$ 中一切室属于 Σ'. 由 ρ 之定义, 对任一 $B \in \Sigma'$, B^ρ 由 Σ' 到 Σ 的一个同构对应所给出. 这一同构保持 C 的一切顶点不变, 故 $\mathbf{G}^\rho$ 为一最短廊. □

定理 3.4 设 $(\Delta, \mathcal{A})$ 为一厦, $\Sigma \in \mathcal{A}$. 则 Σ 为一 Coxeter 复形.

证 由厦之定义, 我们仅需证: 若 C 和 C' 为 Σ 中任意一对相邻的室, 必可找到 Σ 上的迭合 φ, 使 $C'^\varphi = C$.

设 $B = C \cap C'$, 由于 Δ 为厚的, 必可找到包含 B 的室 C'': $C \neq C'' \neq C'$. 令 Σ' 为同时包含 C 和 C'' 的寓,

$$\rho_1 = \text{retr } (\Sigma', C), \rho_2 = \text{retr } (\Sigma, C'),$$

$$\varphi = \rho_1\rho_2 : \Sigma \to \Sigma.$$

以下我们证明, φ 即为所求的迭合. 首先注意, 由定理 3.3(2) 及 φ 的定义, φ 具有如下性质:

(*) 令 $\mathbf{G}$ 为连接 B 和 Σ 中室 D 的长为 $n = \text{dist } BD$ 的廊, 则 $d(B, D^\varphi) = n$, 且 $\mathbf{G}^\varphi$ 为连接 B 和 D^φ 的长为 n 的廊.

由于 C'^φ 包含 B, 则因 Σ 为薄的, 必有 $C'^\varphi = C$ 或 C'. 显然 $\rho_1 : \Sigma \to \Sigma'$ 为 Σ 到 Σ' 的同构, 且 ρ_1 在 C 上平凡作用. 由于 $C'^{\rho_1} \neq C'$, 故 $C'^\varphi = C'^{\rho_1\rho_2} \neq C'$, 这就迫使 $C'^\varphi = C$.

类似地, 可定义 Σ 上态射 φ', 使 φ' 在 C' 上平凡作用. 故有 $C^{\varphi'} = C'$. 令 $D \in \text{Cham } \Sigma$, $\mathbf{G} = (C_0, C_1, \cdots, C_n)$ 为连接 B 和 D 的廊, 其中 $C_0 = C$ 或 C'.

若 $C_0 = C$, 我们证明: (i) φ 和 $\varphi'\varphi$ 均在 D 上平凡作用; (ii) $D^{\varphi'} \neq D$.

假定 $\mathbf{G}$ 为长度极小反例, 且 $\mathbf{G}$ 的长度为 n. 由于 $C^{\varphi'} \neq C$, $C'^\varphi = C$, φ 在 C 上平凡作用, 故有 $n > 0$. 记 $E = C_{n-1}$, 则 $(C_0, \cdots, E)$ 为连接 B 和 E 的长为 $n-1$ 的廊. 由 n 的极小性可知, 对 E, (i) 和 (ii) 均成立. 令 $A = E \cap D$. 因 $A = A^\varphi \subseteq D^\varphi$,

故 $D^\varphi = D$ 或 E. 又由 (*), dist $BD^\varphi = n$, dist $BE = n-1$. 故有 $D^\varphi = D$. 由于 φ 和 φ' 均能使 (*) 成立, 故 $\varphi'\varphi$ 也能使 (*) 成立. 又因 $\varphi'\varphi$ 在 E 上平凡作用, 故 $D^{\varphi'\varphi} = D$, 这就证明了 (i) 成立.

下面证明 (ii). 由于 $\mathbf{G}' = \mathbf{G}^{\varphi'}$ 为一长度为 n 的廊, 且 $C_0^{\varphi'} = C^{\varphi'} = C'$. 由 C 和 C' 的对称性, φ' 在 $D^{\varphi'}$ 上平凡作用. 若 $D = D^{\varphi'}$, 则有 $A = A^{\varphi'} \subseteq D \cap E^{\varphi'}$. 由于 dist $BE^{\varphi'} = n - 1 \neq$ dist BD, 即得矛盾. 这就证明了 $D^{\varphi'} \neq D$.

由以上讨论可知, 或者 $C_0 = C$, $D = D^\varphi$; 或者 $C_0 = C'$, $C_0^\varphi = C$. 通过考察廊 $\mathbf{G}^\varphi$ 可知总有 $D^{\varphi^2} = (D^\varphi)^\varphi = D^\varphi$, 这表明 $\varphi^2 = \varphi$.

又若 $D = D^\varphi$, 则 $D \neq D^{\varphi'}$, $D = D^{\varphi'\varphi}$. 令 $D' \in \Sigma, D' \neq D$, 且 $D'^\varphi = D$, 则 $D^{\varphi'} = D'^{\varphi\varphi'}$. 这意味着 $D^{\varphi'} = D'$. 即 $\{D, D^{\varphi'}\}$ 为 D 关于 φ 的原像集. 这就证明了 φ 为一迭合. □

设 Σ 为厦 Δ 中一个复形, 则 Σ 为 Coxeter 复形. 故 Σ 可用 D-图表示. 由于 Δ 中所有的寓互相同构, 因此, Σ 的 D-图也说是 Δ 的一个 D-图. 以下我们将考察 Δ 与 Σ 的 D-图间的关系. 我们将看到, 厦 Δ 的分类可以通过相应 D-图的分类来实现.

定理 3.5 *I 上厦 Δ 的任意 D-图 $M = (m_{ij})_{i,j\in I}$ 完全由复形 Δ 确定.*

我们先证明如下的引理.

引理 3.6 *令 $(\Delta, \mathcal{A})$ 为一厦, $A \in \Delta$. 我们以 $\mathcal{A}'$ 表示 Δ 中所有包含 A 的寓之集合与 st A 的交, 则 (st $A, \mathcal{A}'$) 为一厦. 我们在 Δ 的 D-图中去掉所有属于 A^τ 的顶点, 所留下的图便是 (st $A, \mathcal{A}'$) 的 D-图.*

证 直接验证表明, (st $A, \mathcal{A}'$) 为一厦. 关于 D-图的结论是显然的. □

定理 3.5 之证明 由室复形中室的定义可知, $\forall C \in$ Cham Δ, 必有 $C^\tau = I$. 令 $i, j \in I$, $A \subset C, A^\tau = I\backslash\{i, j\}$. 则由引理 3.6 和定

理 2.18 可知，st A 中两个室的极大距离为 Δ 的 D-图中的 m_{ij}. □

由定理 3.5 可知，我们可以把 $(\Delta, \mathcal{A})$ 中某个寓 Σ 的 D-图称为 Δ 的 D-图.

定义 3.7 Coxeter 复形 Σ 的子复形 Λ 说是一个凸子复形 (convex subcomplex)，若 $\forall A \in \Lambda, B \in \text{Cham}\ \Lambda$，则连接 A 和 B 的最短廊 $\mathbf{G}$ 中每一项必属于 Λ.

命题 3.8 令 Λ 为寓 Σ 的一个子集，则下列性质等价：

(1) Λ 为凸子复形；

(2) Λ 为某些根之交 (根的定义见 2.11)；

(3) Λ 为 Σ 在某个幂等态射下的像；

(4) 若 $\mathbf{G}$ 为连接 $A \in \Lambda$ 与 $B \in \text{Cham}\ \Lambda$ 的最短廊，则 $\mathbf{G}$ 中每一项均属于 Λ.

证 (1) $\Longrightarrow$ (2)：我们仅需证，若 $A \notin \Lambda$，则有迭合 φ 使 $\Lambda \subseteq \Sigma^{\varphi}$，但 $A^{\varphi} \neq A$. 注意后一条件表明 $A \notin \Sigma^{\varphi}$.

令 $\mathbf{G} = (C_0, \cdots, C_m)$ 为连接 C_0 和 C_m 的廊，其中 $A \subset C_0$，$C_m \in \Lambda$ 且 $\mathbf{G}$ 为满足以上条件的最短廊. 由此可得 $C_{m-1} \notin \Lambda$.

作 C_{m-1} 到 C_m 的迭合 φ. 我们断言 φ 即为所求的迭合.

我们先证 $\Lambda \subseteq \Sigma^{\varphi}$. 为此只需证：若 $C'' \in \text{Cham}\ \Lambda$，则 $C'' \in \Sigma^{\varphi}$. 假定相反，考虑 B, C'' 之间的最短廊，其中 $B = C_{m-1} \cap C_m$，可证

$$\text{dist}\ C_{m-1}C'' = \text{dist}\ C_m C'' - 1.$$

注意由于 C'' 到 C_m 间有一通过 C_{m-1} 的最短廊. 故有 $C_{m-1} \in \Lambda$，矛盾.

我们还须证 $A^{\varphi} \neq A$. 假定相反，则廊

$$\mathbf{G}^{\varphi} = (C_0^{\varphi}, C_1^{\varphi}, \cdots, C_{m-1}^{\varphi} = C_m)$$

为一长度小于 m 的连接 A 和 C_m 的廊，与假定矛盾. 这就证明了 Λ 为 Σ 的某些根之交.

(2) $\Longrightarrow$ (3): 设 $\Lambda = \bigcap_{i\in J}\Sigma^{\varphi_i}$, $J=\{1,2,\cdots,m\}$. 令 $\psi = \prod_{i=1}^{m}\varphi_i$. 则直接验证表明 $\Lambda=\Sigma^{\psi}$.

(3) $\Longrightarrow$ (4): 令 $\Lambda=\Sigma^{\psi}$, ψ 为 (3) 中所定义的幂等态射. 令 $\mathbf{G}$ 为连接 $A\in\Lambda$ 和 $C\in \mathrm{Cham}\ \Lambda$ 的最短廊. 由于 $A^{\psi}=A$, $C^{\psi}=C$, 则 $\mathbf{G}^{\psi}$ 仍是连接 A 和 C 的最短廊, 且对于 $\mathbf{G}$ 中任意项 C',

$$\mathrm{dist}\ C'^{\psi}C=\mathrm{dist}\ C'C.$$

由此可知, $C'\in\Sigma^{\psi}=\Lambda$.

(4) $\Longrightarrow$ (1): 显然. □

命题 3.9 *令 A, B 属于寓 Σ, Λ 为包含 $\{A,B\}$ 的极小凸子复形. 则 $\mathrm{st}\ A\cap\Lambda$ 中有最大元 A'. 若 $B\in\mathrm{Cham}\ \Sigma$, 则 $A'\in\mathrm{Cham}\ \Sigma$ 且 A' 为连接 A 与 B 的最短廊中第一项.*

证　先假定 B 为一室. 则由命题 3.8(4), A 到 B 的最短廊中所有的项均属于 Λ. 特别地, $\mathrm{Cham\ st}\ A\cap\Lambda$ 中包含一个室 A'. 我们断言, $\forall D\in\mathrm{st}\ A\cap\Lambda$, 必有 $D\subset A'$. 假定相反, 令 $\varphi,\bar\varphi$ 为相对的迭合, 使 $D\notin\Sigma^{\varphi}$, $A'\notin\Sigma^{\bar\varphi}$. 则有 $D\in\Sigma^{\bar\varphi}$, $A'\in\Sigma^{\varphi}$, $A\in\Sigma^{\varphi}\cap\Sigma^{\bar\varphi}$. 从而若 $B\in\Sigma^{\varphi}$, 便有 $\Lambda\subseteq\Sigma^{\varphi}$; 而若 $B\in\Sigma^{\bar\varphi}$, 则有 $\Lambda\subseteq\Sigma^{\bar\varphi}$. 以上两种情况均与假定 $\{A',D\}\subseteq\Lambda$ 相矛盾.

若 B 为 Σ 中任意元, 假定 C 为包含 B 的室. 由前面的证明可知, 存在室 $A''\in\mathrm{st}\ A$, 能使 A'' 为 $\Lambda\cap\mathrm{st}\ A$ 中最大元, 这里 Λ 为任意包含 $\{A,C\}$ 的凸子复形, 由此立得结论. □

命题 3.10 *令 Σ 为厦 Δ 中一寓, $C,D\in\mathrm{Cham}\ \Delta$. 假定恰有两个廊连接 C 和 D, 这两个廊除 C,D 外, 无其它公共元. 则 $C\cap D=A$ 的余维数为 2, 且上述两个廊中室集合恰为 $\mathrm{Cham\ st}\ A$.*

证　令 $\mathbf{G}=(C,C_1,\cdots,D)$ 和 $\mathbf{G}'=(C,C_1',\cdots,D)$ 为所说的两个廊. 令 $B=C\cap C_1\cap C_1'$. 由假定, $\mathbf{G}_1=(C_1,\cdots,D)$ 为连接 C_1 和 D 的唯一的最短廊. 令 Λ 为包含 $\{C_1,D\}$ 的极小凸子复形. 由命题 3.8, $\mathrm{Cham}\ \Lambda$ 等于 $\mathbf{G}_1$ 中所有室之集合. 又由命题 3.9, $\Lambda\cap\mathrm{st}\ B$ 中包含最大元 E. 这表明 E 为 $\mathbf{G}_1$ 中一项. 同理, 若 Λ'

为包含 $\{C_1', D\}$ 的极小凸子复形，则 $\Lambda' \cap \mathrm{st}\ B$ 中包含最大元 E'，且 E' 为廊 $(C_1', \cdots, D)$ 中的一项，这就迫使 $E = E' = D$. 特别地， $B \subset D$. 从而 st B 为一秩 2 的 Coxeter 复形，再由定理 2.18, 命题得证. □

定理 3.11 令 $(\Delta, \mathcal{A})$ 和 $(\Delta', \mathcal{A}')$ 为两个厦. 令 $\varphi: \mathrm{Cham}\ \Delta \to \mathrm{Cham}\ \Delta'$ 为保持邻接关系的 1-1 映射. 则 φ 可唯一地扩充为 Δ 到 Δ' 的同构.

证 由假定, 两个室 C, D 相邻接当且仅当 C^φ, D^φ 相邻接.

设 $A \in \Delta$, codim $A = 1$, 则 Cham st A 中所有室互相邻接，且 Cham st A 为具有这种性质的极大集合. 因此 (Cham st $A)^\varphi$ 也是一个由两两相互邻接的室构成的极大集合.

我们说,这时必有 $A' \in \Delta'$, codim $A' = 1$, 能使 (Cham st $A)^\varphi =$ Cham st A'.

为证上述论断, 仅需注意由于 (Cham st $A)^\varphi$ 中所有室互相邻接，故其任意两室的交必为唯一确定的单形 A'. 记 $A^\varphi = A'$. 由命题 3.10 可知，室集合 L 为 st $(A \cap B)$ 中一个寓中全体室的集合，当且仅当存在 $D \in L$ 具有下列性质：恰有两个最短廊连接 C 和 D, 这两个廊除 C, D 外无其它公共室，且它们由 C 出发的第二项分别属于 st A 和 st B.

由于厦 st $(A \cap B)$ 为它们的寓的并，这样我们就利用邻接关系对 Cham st A 进行了刻划. 特别地，我们有

$$(\mathrm{Cham\ st}\ (A \cap B))^\varphi = \mathrm{Cham\ st}\ (A^\varphi \cap B^\varphi). \tag{3.1}$$

对于 $C \in \mathrm{Cham}\ \Delta$, 定义 I 到 I' 的同构 $\widetilde{\varphi_C}$ 如下： $\forall A \subset C$, codim $A = 1$, 令 $(A^\tau)^{\widetilde{\varphi_C}} = (A^\varphi)^{\tau'}$.

现假定 $C, D \in \mathrm{Cham}\ \Delta$ 相邻接, 令 $E = C \cap D$, $A \subset C$, $B \subset D$, 且 codim $A = 1 =$ codim B. 则成立

$$A^\tau = B^\tau \iff \mathrm{Cham\ st}\ (A \cap E) = \mathrm{Cham\ st}\ (B \cap E).$$

从而由 (3.1) 式可知

$$A^\tau = B^\tau \iff (A^\varphi)^{\tau'} = (B^\varphi)^{\tau'}.$$

这表明 $\widetilde{\varphi_C} = \widetilde{\varphi_D}$. 这一结论对于任意二个相邻室均成立，故由 Δ 的连通性可知，$\widetilde{\varphi_C}$ 与 C 的选择无关. 记 $\widetilde{\varphi_C} = \varphi$.

令 $J \subseteq I$, 则对于 $C, D \in \text{Cham}\ \Delta$, $C \cap D$ 中包含型为 J 的面 $\iff$ 存在廊 $C = C_0, C_1, \cdots, C_m = D$, 能使 $J \subseteq (C_i \cap C_{i+1})^\tau$, $\forall i \in \{0, 1, \cdots, m-1\}$. 由 φ 之定义，$C \cap D$ 中包含 J 型面 $\iff$ $C^\varphi \cap D^\varphi$ 中包含 J^φ 型面. 这就证明了定理. □

§4. BN-对

BN-对的概念与厦的概念密切相关. 可以说 BN-对是厦的代数实现，而厦刻画了 BN-对的几何结构.

我们在本节证明，由任一 BN-对出发，可以构造一个厦，反之，任一厦的满足某些条件的自同构群为 BN-对. 由于任一 Lie 型群都具有 BN-对结构，因此 Lie 型群的分类问题便可以转化为 BN-对的分类. Tits 还证明了秩 ≥ 3 的有限 BN-对必为 Lie 型群的 BN-对，关于秩小于 3 的 BN-对也有许多结果. 但也必须指出，厦与 BN-对这两个概念并非完全等价的，每一 BN-对都可以看作一个厦的满足某些条件的自同构群，但并非每一厦都可由 BN-对出发构造出来. 在本节末，我们还将看到，不同的 BN-对可能构造出同一厦.

定义 4.1 令 G 为一群，G 的二个子群 B 和 N 说是一个 BN-对, 若下列条件成立:

(T1) $G = \langle B, N \rangle$, $B \cap N \trianglelefteq N$;

(T2) 群 $W = N/B \cap N$ 有一个 2 阶元的生成元集合 S;

(T3) $\forall s \in S$, $w \in W$, 成立: $sBw \subseteq BwB \cup BswB$;

(T4) 对任意的 $s \in S$, 总有 $sBs \not\subseteq B$.

满足 (T1)-(T4) 的四元组 (G, B, N, S) 叫做一个 Tits 系 (Tits system), W 叫做这一 Tits 系的 Weyl 群.

在进一步讨论之前，我们先对定义 4.1(T3) 和 (T4) 中的一些记法，如 sBw, BwB 等加以说明. 注意 s, w 均为 N 中元素关于 $N \cap B$ 的陪集. 令 $s = \tilde{s}(B \cap N), w = \tilde{w}(B \cap N) = (B \cap N)\tilde{w}$, 其

中 $\tilde{s}$ 和 $\tilde{w}$ 分别为 s 和 w 在 N 中的代表元，我们把 sBw 理解为 G 的子集 $\tilde{s}B\tilde{w}$.

下面我们给出一个 Tits 系的例子.

例 4.2 令 $\mathbf{F}=GF(q)$, $G=GL(n,q)$, 即 G 为 $\mathbf{F}$ 上全体 n 级可逆矩阵之集合. 以 $\mathbf{E}_{ij}$ 表示 (i,j) 元为 1, 其他元均为 0 的 n 级矩阵. 令

$$T=\langle I+a_{ij}\mathbf{E}_{ij}\;\big|\;a_{ij}\in F,1\le i<j\le n\rangle;$$

$$H=\langle I+(a_{ii}-1)\mathbf{E}_{ii}\;\big|\;a_{ii}\in F^{\#},1\le i\le n\rangle;$$

$$K=\langle I-\mathbf{E}_{ii}-\mathbf{E}_{jj}+\mathbf{E}_{ij}+\mathbf{E}_{ji}\;\big|\;1\le i\le n,1\le j\le n\rangle.$$

易知 $T\in \mathrm{Syl}_p(G)$, $N_G(T)=TH$, $N_G(H)=HK$. 记 $B=TH,N=HK$. 显然 $B\cap N=H\trianglelefteq N$. 直接验证表明： B,N 为 G 中一个 BN-对.

定理 4.3 令 $\Delta=(\Delta,\mathcal{A})$ 为一厦， $\Sigma\in\mathcal{A}$, C 为 Σ 中一个室. 设 $G\le \mathrm{Aut}(\Delta)$, 且满足下列条件:

(A1) 若 Σ' 为 Δ 的寓， C' 为 Σ' 中一个室，则有 $\sigma\in G$ 能使 $\Sigma^\sigma=\Sigma'$, 且 $C^\sigma=C'$.

令 $B=N_G(C)=\{g\in G\mid C^g=C\},N=N_G(\Sigma)=\{g\in G\mid \Sigma^g=\Sigma\}$, S 为 Σ 的关于 C 的所有墙的反射之集合. 则 (G,B,N,S) 为一 Tits 系.

证 由条件 (A1), G 在 Δ 中寓的集合和室的集合上都传递. 由于 $N=N_G(\Sigma)$, 故任意 $\sigma\in N$ 导出 Σ 的一个自同构，记作 σ^ω. 显然 σ^ω 为 Σ 的 Weyl 群 W 中的一个元. 从而 $\omega:\sigma\mapsto\sigma^\omega$ 为 N 到 W 的一个同态对应. ω 的核固定室 C, 则由于 W 为正则，便有 $\mathrm{Ker}\,(\omega)=B\cap N\trianglelefteq N$.

对于 $g\in G$, C^g 为一室. 可找到 Σ' 同时包含 C 和 C^g. 由条件 (A1) 知, 可找到 $b\in G$ 把 (Σ,C) 同构地映到 (Σ',C). 显然 $b\in B$. 因 $C^g\in\Sigma'$, 故 $(C^g)^{b^{-1}}\in\Sigma$. 又因 W 在 Σ 上传递, 且 $N^\omega=W$, 故有 $n\in N$, 能使 $(C^g)^{b^{-1}n^{-1}}=C$. 故有 $b_1=gb^{-1}n^{-1}\in B$. 从而得 $g=b_1nb$, 这表明 $G=\langle B,N\rangle$, 更确切地说, 有 $G=BNB$. 这样就证明了 (T1),(T2).

以下证明 (T3). 注意, 若 $n\in N$, 则 C^n 所表示的室恰是 C^{n^ω}, 故我们记 $C^{n^\omega}=C^n$. 令 $s\in S, w\in W$, 则 C 与 C^s 相邻, 即 $D=C\cap C^s$ 为一墙. 若 $b\in B$, 则 b 固定 C 的任意顶点, 故 $(C^s)^b$ 包含 D, $((C^s)^b)^w$ 包含 D^w. 由 (B3), 有寓 Σ' 同时包含 C 和 C^{sbw}. 令 $\mathbf{G}=(C_0=D^w,C_1,\cdots,C_m=C)$ 为连接 D^w 和 C 的最短廊, 由于 D^w 和 C 都既包含在 Σ 中又包含在 Σ' 中, 从而所有的 C_i 都属于 $\Sigma\cap\Sigma'$. 由条件 (A1), 有 $b'\in\mathbf{G}$, b' 将 (Σ',C) 变到 (Σ,C). 故 $C^{b'}=C$, 从而 $b'\in B$. 由于 b' 固定 C 的任意顶点, 故 b' 固定 $E=C_{m-1}\cap C_m$, 即 $C_{m-1}^{b'}$ 是包含 E 的室. 由于 Σ 为薄的, 便有 $C_{m-1}^{b'}=C_{m-1}$. 故 b' 固定 C_{m-1} 的一切顶点. 重复以上过程, 可知 b' 固定 C_0 的一切面. 特别地, b' 固定 D^w.

由以上讨论可知: $D^w\subset C^{sbw}$ 且 C^{sbw} 为 Σ' 的一室. 由于 $D^{wb'}=D^w$, 便得 $D^w=D^{wb'}\subset C^{sbwb'}\in\Sigma'^{b'}=\Sigma$. 因为 Σ 为一寓, 故恰有 Σ 的两个室 C^w 和 C^{sw} 同时包含 D^w. 由此便得: $C^{sbwb'}=C^w$ 或 $C^{bswb'}=C^{sw}$. 从而有 $sbw\in BwB\cup BswB$, 即 (T3) 成立.

最后我们证明 (T4). 如前令 $D=C\cap C^s$, 则由于 Δ 为厚的, 便可找到 $C'\neq C$ 或 C^s, 且能使 $D\subset C'$. 令 Σ' 同时包含 C 和 C', 则有 $b\in G$ 把 (Σ,C) 映到 (Σ',C). 故 $b\in B$, C^{sb} 为 Σ' 中包含 D 的室. 故必有 $C^{sb}=C'$. 因 $C'\neq C^s$, 便得 $sbs\notin B$, 这就证明了 (T4). □

以下我们将证明上述定理之逆, 即任一个带有 BN-对的群 G, 可以看作是一个厦的自同构群, 且对于 G, 定理 4.3 中的条件 (A1) 成立. 为此我们需要带有 BN-对的群的若干基本性质.

设 w 为 $n\in N$ 关于 $N\cap B$ 的陪集, 记 $C(w)=BwB=BnB$.

利用上述记法, (T3) 可以写做: $C(s)C(w) \subseteq C(w) \cup C(sw)$. 由此可得: $C(w)C(s) \subseteq C(w) \cup C(ws)$. 一般地, 若 $s_1, s_2, \cdots, s_n \in S$, 则成立:

(A2) $C(s_1 \cdots s_n)C(w) \subseteq \bigcup_{i=1}^n C(s_i \cdots s_n w)$.

取 $J \subseteq S$ 并令

$$W_J = \langle J \rangle, P_J = BW_J B.$$

由 (A2) 可推知, P_J 为 G 的子群, $P_J \supset B$. 又显然有 $W_S = W$ 且 $G = BWB$. G 的一个子群 K 说是一个 (关于 BN-对) 的*抛物子群* (Parabolic subgroup), 若它与某个 P_J 共轭. 设 $|S| = m$, 若 $|J| = r$, 则 G 中恰有 2^{m-r} 个包含 P_J 的抛物子群. 若 $|J| = 1$, 则 P_J 叫做极小抛物子群.

以下我们证明, G 的任一包含 B 的子群必为某个 P_J. 令 W 为 Tits 系 (G, B, N, S) 的 Weyl 群. 对任意 $w \in W$, 有 $w = s_1 \cdots s_n$, $s_i \in S$. 这一表达式不是唯一的. w 的如上表达式中最短表达式中之因子个数说是 w 的长度, 并记作 $l(w)$. 下文中, w, w' 总表示 W 中的元, 而 $s, s_1, \cdots$ 表示生成元集 S 中的元.

命题 4.4 (1) 由 $C(w) = C(w')$ 可得 $w = w'$, 由此可知 B 在 G 中的二重陪集与 W 的元成 1-1 对应;

(2) 若 $l(sw) \geq l(w)$, 可得 $sBw \subseteq C(sw)$;

(3) 若 $l(sw) \leq l(w)$, 则 $sBw \cap BwB \neq \varnothing$;

(4) 令 $l = l(w)$, 且 $w = s_1 s_2 \cdots s_l$ 为 w 的最短表达式, 则对任意的 i, 有 $s_i B \subseteq \langle B, wBw^{-1} \rangle$. 进而, 有 $C(w) \subseteq \langle B, wBw^{-1} \rangle$.

证 (1) 假定 $l(w) \leq l(w')$, 并对 $l = l(w)$ 施行归纳. 若 $l = 0$, 则 $w = 1$. 这时有 $C(w) = B = C(w')$. 从而 $w' = 1$. 现假定 $l(w) = l > 0$. 设 $w = sw''$, 其中 $l(w'') = l - 1$. 由假定, 有 $sw''B \subseteq C(w')$. 则由 (T3)

$$w''B \subseteq sBw'B \subseteq C(w') \cup C(sw').$$

这表明 $C(w'') = C(w')$ 或 $C(w'') = C(sw')$. 由归纳假定，得 $w'' = w'$ 或 $w'' = sw'$. 但因 $l(w') \geq l$, 故 $w'' = w'$ 不可能成立，从而有 $w'' = sw'$, 即有 $w' = sw'' = w$.

(2) 仍对 $l = l(w)$ 施行归纳. 记 $w = w'r$, 其中 $l(w') = l - 1$, 且 $r \in S$. 若 $l(sw') < l - 1$, 则有 $l(sw) = l(sw'r) < l$. 这与假定 $l(sw) \geq l$ 相矛盾，故成立 $l(sw') \geq l - 1$. 由归纳假定 $sBw' \subseteq C(sw')$. 故

$$sBw = sBw'r \subseteq C(sw')C(r) \subseteq C(sw') \cup C(sw'r) = C(sw') \cup C(sw).$$

另一方面，(T3) 表明 $sBw \subseteq C(w) \cup C(sw)$. 若 $C(w)$ 与 $C(sw')$ 有一公共元，则由 (1) $w = sw'$, 便得 $l(sw) = l(w') = l - 1$, 矛盾. 这就得出 $C(w) \cap C(sw') = \varnothing$, 从而成立 $sBw \subseteq C(sw)$.

(3) 由 (T3) 和 (T4), 得 $sBs \cap BsB \neq \varnothing$, 故

$$sBsw \cap BsBw \neq \varnothing, \forall w \in W.$$

由假定，若令 $sw = w'$, 则有 $l(sw') \geq l(w')$. 故由 (2), $sBw' \subseteq C(sw')$. 因 $sw' = w$, 便有 $BwB \cap BsBw \neq \varnothing$, 即 $BwB \cap sBw \neq \varnothing$.

(4) 由假定，$l(s_1 w) < l(w)$. 故由 (3) 可得 $s_1 Bw \cap BwB \neq \varnothing$. 这表明

$$s_1 B \subseteq BwBw^{-1}B \subseteq \langle B, wBw^{-1} \rangle.$$

对 $w_1 = s_1 w$ 及 s_2 重复以上讨论过程便得：

$$s_2 B \subseteq \langle B, w_1 B w_1^{-1} \rangle \subseteq \langle B, wBw^{-1}, s_1 \rangle = \langle B, wBw^{-1} \rangle.$$

重复这一过程可得 $s_i B \subseteq \langle B, wBw^{-1} \rangle$. 这样我们便证明了 (4). □

定理 4.5 令 (G, B, N, S) 为一 Tits 系.

(1) 包含 B 的子群 P 确定 S 的一个子集 J, 使得 $P = P_J$, 其中 $J = \{s \mid s \in S, C(s) \subset P\}$.

(2) 设 $g \in G$. 由 $B^g \subset P_J$ 可得 $g \in P_J$. 又对任意 P_J, 成立 $N_G(P_J) = P_J$. 进而，若 P_J 与 P_K 在 G 中共轭，必有 $P_J = P_K$.

(3) 令 J 与 K 均为 S 的子集，$I = J \cap K$. 则有 $P_I = P_J \cap P_K$. 从而 G 的包含 B 的子群格 $\{P_J \mid J \subseteq S\}$ 同构于 S 的子集格 $\{J \mid J \subseteq S\}$.

证 (1) 显然 P 是 B 的二重陪集的并，即 $P = \bigcup_{n \in P} BnB$. 假定 $C(w_\alpha) \subset P$, 且

$$w_\alpha = s_1^{(\alpha)} s_2^{(\alpha)} \cdots s_{n_\alpha}^{(\alpha)}$$

为相应的最短表达式，则

$$C(s_i^{(\alpha)}) \subset \langle B, C(w_\alpha) \rangle \leq P.$$

令 $J_\alpha = \{s_1^{(\alpha)}, \cdots, s_{n_\alpha}^{(\alpha)}\}$, 则 $P_{J_\alpha} \leq P$. 从而成立 $P = P_J$, 其中 $J = \bigcup J_\alpha$.

(2) 因 $G = BWB$, 则 g^{-1} 必属于某一 $C(w)$, 其中 $w \in W$. 由假定 $B^g \leq P_J$, 故 $wBw^{-1} \leq P_J$. 从而 $C(w) \subseteq \langle B, wBw^{-1} \rangle \leq P_J$, 即得 $g \in P_J$. 其他结论可用类似的方法得出.

(3) 首先证明 S 为 W 之一极小生成元集. 假定相反，即假定 $W = \langle s \mid s \in S \backslash \{s_i\} \rangle$, $s_i \in S$. 易知 $(G, B, N, S\backslash\{s_i\})$ 仍为一 Tits 系. 设 $s_i = s_{j_1} \cdots s_{j_t}$, $s_{j_l} \in S\backslash\{s_i\}$ 为 s_i 在 $(G, B, N, S\backslash\{s_i\})$ 中的最短表达式. 则由命题 4.4(4), 有 $s_{j_l}B \subseteq \langle B, s_iBs_i \rangle \leq \langle B, s_i \rangle = B \cup Bs_iB$. 从而有 $s_{j_l}B \subset Bs_iB$. 故有 $Bs_{j_l}B = Bs_iB$. 又由命题 4.4(1), 即得 $s_{j_l} = s_i$, 矛盾.

现令 J, K 为 S 的两个子集. 因 $P_J \cap P_K$ 为 G 的包含 B 的子群，所以 $P_J \cap P_K = P_L$, 其中 $L \subseteq S$. 显然 $P_I = P_{J \cap K} \leq P_L$. 假定 $P_I < P_L$, 则 $I \subset L$. 不失一般性，可假定 $L \not\subset J$. 由 $P_L \leq P_J$ 可知 $W_L \leq W_J$. 设 $s_i \in L\backslash J$, 则 s_i 可由 J 中元表出，而这是不可能的，故有 $P_J \cap P_K = P_{J \cap K}$.

最后，我们证明由 $P_J = P_K$ 可推得 $J = K$. 若 $J \neq K$, 则可假定 $J\backslash K$ 非空. 因 $P_J = P_J \cap P_K = P_{J \cap K}$, 故 $W_J = W_{J \cap K}$. 这表明有某一 s_i 可由其余生成元表示，矛盾. 这就证明了结论. □

定理 4.6 . 令 (G, B, N, S) 为一 Tits 系，$\Delta = \{Pg \mid B \leq P \leq G, g \in G\}$. 在 Δ 上定义序关系如下：对 Δ 中任意两个陪集 Pg 和

$P'g'$, 规定 $Pg \prec P'g'$, 当且仅当 $P'g'$ 为 Pg 的子集. 令

$$\Sigma = \{Pn \mid P \geq B, n \in N\}.$$

令 $\mathcal{A} = \{\Sigma g \mid g \in G\}$, 则 $(\Delta, \mathcal{A})$ 为一厦, 其中 B 的陪集为室. 又两个元 Pg 和 $P'g'$ 有相同的型, 当且仅当 $P = P'$. 群 G 通过右乘作用在 Δ 上, 由 G 的全体元素所导出的 Δ 的自同构群满足定理 4.3 中的条件 (A1). S 为关于室 B 中所有墙的反射之集合. G 在 Δ 上作用的作用核记作 $\ker_B(G)$.

证　先证明 Δ 为一秩为 $|S| = d$ 的室复形.

注意, 下文中, 群 G 中元素 g 右乘 Δ 中的对象 (子群陪集或陪集集合) 时, 既表示 g 同该对象相乘, 又表示 g 作为自同构的作用.

首先, Bg 为 Δ 的极大元. 由于右乘作用为 Δ 上的自同构, 故仅需证明 B 为极大元即可. 假定 $B \prec Pg$, 则 $Pg \subseteq B$. 从而 $g \in B$, 故 $P \subseteq B$. 这表明 $Pg = B$, 即 B 为极大元.

现考虑集合 $[B] = \{Pg \mid Pg \prec B\}$. 易知 $Pg \in [B]$ 当且仅当 B 为 Pg 之子集. 这时 $Pg = P$ 为 G 的包含 B 的子群. 由于 $P = P_J$, 其中 J 为 S 的某个子集, 故 $[B]$ 中任意元对应于 S 的唯一确定的子集 J. 又 $P_J \prec P_K \iff K \subset J$. 故 B 为一 d 秩单形. 又 Δ 中任意两个元 Pg 与 P' 有极大公共下界 $P'' = \langle P', Pg\rangle$, 这就表明 Δ 为一 d 秩复形.

以下证明 Σ 为 Δ 的秩 d 子复形. 设 $P'g' \prec Pn$, 则 $Pn \subseteq P'g'$. 从而 $n \in P'g'$, $P'g' = P'n \in \Sigma$. 故 Σ 为一子复形. 因 $Pn \prec Bn$, 故 Σ 为 Δ 的秩 d 子复形. 由于 Σ 中余维数为 1 的元为子群 $P = \langle B, s\rangle, s \in S$, 故 $P \prec Bg \iff g \in B \cup BsB$. 从而有 $g = 1$ 或 $g = s$. 这表明 $P = \langle B, s\rangle$ 仅包含在极大元 B 和 Bs 之中.

另一方面, 因 $sB \neq Bs$, 故 $|P : B| \geq 3$, 从而 Δ 中任一余维数为 1 的元至少包含在 3 个极大元之中. 对于 Σ 中的极大元 B 和 Bw, 其中 $w = s_1 \cdots s_n$ 为 w 在 W 中的最短表达式, 序列 $(B, Bs_n, Bs_{n-1}s_n, \cdots, Bs_1 \cdots s_n)$ 为连接 B 和 Bw 的廊. 这就证明了 Σ 是连通的. 故 Σ 为薄 (室) 复形, 即 (B2) 成立.

令 Pg 和 $P'g'$ 为 Δ 的两个元. 因 $G = BWB$, 故可找到 $b, b' \in B$ 及 $n \in N$, 使 $g'g^{-1} = bnb'$. 从而 $Pg = Pb'g, P'g' = P'nb'g$. 这表明 Pg 和 $P'g'$ 同属于 $\Sigma b'g \in \mathcal{A}$. 这就证明了 (B3). 由此及 Σ 的连通性, 可知 Δ 也是连通的. 这就表明 Δ 为一厚 (室) 复形, 即 (B1) 成立.

最后, 我们证明 (B4). 令 $\Sigma = \{Pn \mid n \in N\}$. 假定 $\Sigma' = \Sigma g$ 包含 Pn 和 $P'n'$. 我们证明可找到 $x \in G$, 使得 $\Sigma x = \Sigma g$, 且 x 保持 Pn 和 $P'n'$ 不变.

由定义, 有 $m, m' \in N$ 能使 $Pn = Pmg$ 且 $P'n' = P'm'g$. 令 $g' = m'gn'^{-1}$, 则 $P' = P'g'$, 即 $g' \in P'$. 令 $m'' = mm'^{-1}, n'' = nn'^{-1}$, 则 $Pm''g' = Pn''$. 故 $m'' \in Pn''P'$, 从而有 $m'' = wn''w'$, 其中 $w \in P \cap N, w' \in P' \cap N$. 令 $x = n'^{-1}w'g'n'$, 则

$$Pnx = Pn''n'x = Pn''w'g'n' = Pwn''w'g'n' = Pm''g'n' = Pn,$$

$$P'n'x = P'w'g'n' = P'g'n' = P'n'.$$

又 $\Sigma x = \Sigma n'x = \Sigma w'g'n' = \Sigma m'g = \Sigma g$, 故 $x : \Sigma \mapsto \Sigma g$ 满足所求性质. 这就证明了 Δ 为一厦, 而 $\mathcal{A}$ 为寓之集合. $[B]$ 的元与 Δ 的型集合成 1–1 对应, 故

$$(Pg)^{\tau} = (P'g')^{\tau} \iff P = P'.$$

由定义, G 在寓的集合上的作用是传递的, N 包含在寓 Pn 的一个稳定子之中. Σ 的一切室具有形式 Bn, 故 N 在 Σ 的室集合上传递. 从而 $G \leq \mathrm{Aut}\Delta$, 且 G 满足定理 4.3 中条件 (A1). 其余结论显然成立. □

由定理 4.6, 定理 3.4 和定理 2.16 可知以下事实: 令 $W = N/N \cap B$, 则 (W, S) 为一 Coxeter 系.

在定理 4.6 中室 B 在 G 中的稳定子为 B, 而寓 $\Sigma = \{Pn\}$ 的稳定子为 HN, 其中

$$H = \bigcap_{n \in N} n^{-1}Bn.$$

显然 N 正规化 H, 从而 HN 为 G 的子群. 不难看出, (B,HN) 也为一 BN-对, 且与 (B,N) 定义同一厦. 在 BN-对 (B,N) 中, 若 $H=B\cap N$, 则 (B,N) 说是饱和的. 据此 (B,HN) 为饱和的. 若 (B,N) 为饱和的, 则相应的寓 Σ 的稳定子为 N.

假定群 $G\leq \mathrm{Aut}\Delta$, 且 G 满足定理 4.3 中条件 (A1). 令 Σ 为 Δ 之一寓, C 为 Σ 之一室. 令 $B=N_G(C), N=N_G(\Sigma)$, 则 (G,B,N,S) 为一 Tits 系. 由这一 Tits 系可构造一厦与 Δ 同构. 室 C 中恰包含一个具有特定的型的元. 故对任意的 $A\subset C, A$ 在 G 中的稳定子为包含 B 的子群 P. 令 $D\in\Delta$, 若 D 与 A 在 Δ 中具有相同的型, 则 G 中把 A 变到 D 的元之集合为 $Pg, g\in G$. 从而 $D\mapsto Pg$ 为 Δ 到由 (G,B,N,S) 所定义的厦间的同构对应. 又在定理 4.6 中所定义的寓为以 N 中元为代表元的陪集集合, 对于 N 到 Weyl 群上的自然映射 ω, 命题 4.4(1) 等价于 $(BnB\cap N)^{\omega}=\omega(n)$. 从而有 $(P_Jn\cap N)^{\omega}=W_J^{\omega(n)}$. 故 Σ 的元对应于 W_J 的陪集. 特别地, 因任一寓同构于所有 $W_J(J\subseteq S)$ 在 W 中的陪集所构成的集合, 故寓由 Weyl 群所唯一确定.

利用例 4.2, 我们可以得出 $PSL(n,q)$ 的 BN-对结构, 在习题 2 中, 我们将进一步看到 $PSL(n,q)$ 的 BN-对与例 1.7 中所定义的厦 $\Delta(\mathcal{P})$ 的相互关系.

由下列定理我们可以初步看到 Tits 几何理论与有限单群理论, 特别是 Lie 型群理论的关系.

定理 4.7 设 (G,B,N,S) 为一 Tits 系, 其中 (W,S) 为不可约 Coxeter 系且 $\ker_B(G)=1$. 则

(1) 若 $X\trianglelefteq G$, 则 $G=XB$;

(2) 若 $G'=G$ 且 B 可解, 则 G 为单.

证 令 $X\trianglelefteq G$, 则 $XB\leq G$. 由定理 4.5(1), 存在 $J\subseteq I$, 使 $XB=P_J$. 令

$$J_0=\{i\in I\mid (Bs_iB)\cap X\neq\varnothing\}.$$

若 $i\in J_0$, 则 $s_i\in Bs_iB\subseteq XB=P_J$. 故由定理 4.5(2), $i\in J$. 反之, 由 $P_J=XB$, 故 X 与 B 在 P_J 中的任意陪集均有非空交. 这样

$J \subseteq J_0$. 这就证明了 $J = J_0$. 现在我们证明 $J = I$. 假定相反. 由于 (W,S) 为不可约 Coxeter 系, 则存在 $i \in I \backslash J$ 及 $j \in J$ 使 $[s_i, s_j] \neq 1$. 由于 $\langle s_i, s_j \rangle$ 为二面体群. 故 $l(s_i s_j s_i) > l(s_j s_i) > l(s_i)$, 从而由命题 4.4(2) 可知 $Bs_iBs_jBs_iB = Bs_is_js_iB$. 由于 $X \trianglelefteq G$, $J = J_0$, 故有 $s_is_js_i \in W \cap P_J = W_J$. 这表明 $s_is_js_i \in W_J \cap W_{\{i,j\}} = W_{\{j\}} = \langle s_j \rangle$, 与假定 $[s_i, s_j] \neq 1$ 相矛盾. 故有 $I = J$, 特别地 $XB = P_J = P_I = G$. 这就证明了 (1). (2) 是 (1) 的直接结果. □

注意, 定理 4.7 的结果带有很大的普遍意义. 由于典型群都带有 BN-对结构, 并且满足定理 4.7 的条件, 因此射影典型群的单性可以看作是定理 4.7 的直接结果.

厦和 BN-对的理论有很多很有意义的推广. 下节我们将要介绍的融合理论就是 BN-对理论的推广.

§5. 融合理论

定义 5.1 设 G 为一群, B 为 G 的子群, $\mathcal{P} = \{P_i \mid i \in I\}$ 为群 G 中一个子群族, 其中 $I = \{1, 2, \cdots, n\}, n \geq 2$. 三元系 $(G; (P_i)_{i\in I}; B)$ 说是一个秩 n *抛物系* (parabolic system), 若成立

(1) $G = \langle P_i \mid i \in I \rangle$;

(2) $P_i \cap P_j = B \neq P_j, \forall i, j \in I$, 特别地, $B = \bigcap_{i\in I} P_i$;

(3) $\bigcap_{g\in G} B^g = 1$.

这时下标 i 说是子群 P_i 的型, 子群 B 说是 $\mathcal{P}$ 的 Borel 子群, $P_i, i \in I$ 说是极小抛物子群, n 说是*抛物系的秩* (rank). 群 G 说是子群族 $(P_i)_{i\in I}$ 或*抛物系的完备* (completion).

对于 $J \subset I$, 令 $P_J = \langle P_i \mid i \in J \rangle$. 我们还规定 $P_\varnothing = B$. 子群 P_J 说是 G 中型为 J 的抛物子群. 一般地, 我们考虑秩大于 1 的抛物系. 为了方便起见, 我们规定群 G 中的秩 1 抛物系为一真子群 B 能使 $\cap_{g\in G} B^g = 1$. 由命题 1.5 可知, 利用抛物系 $(G; (P_i)_{i\in I})$, 可以定义一个室复形 $\Delta(G; (P_i)_{i\in I})$, 并从而得到一个室系 $\mathcal{C}(G; (P_i)_{i\in I})$. G 可以看作是相应的复形的自同构群.

注意，在定义抛物系时，我们并未对群 G, B 及 $P_i, i \in I$ 作任何要求，它们都可以是未知的. 但读者由命题 1.5 不难想到 G 中抛物系的存在性，必将对群 G 的结构及 G 与其抛物子群间的相互关系产生一定的影响.

有关抛物系理论的问题常以以下方式提出：设 $(G;(P_i)_{i\in I})$ 为一抛物系，通过一些关于 G 或子群系 $(P_i)_{i\in I}$ 的条件 (通常是群论的或几何的)，得出关于群 G 的一些结论；如果这些条件足够强，我们甚至可以得出 G 的结构，或对所有满足相应条件的群 G 加以分类. 由于所给的群论条件，大多与*局部子群* (local subgroup)，即某个 p-子群的正规化子有关，因此局部子群分析是解决问题的重要途径；又鉴于抛物系与室复形等的关系，几何方法也是考察抛物系的一种强有力的工具. 综合运用两种方法，常常可以得到很好的结果.

秩 2 抛物系和秩 3 抛物系与群论，特别是有限单群理论有着密切关系. 限于篇幅，我们着重介绍解决秩 2 抛物系问题的群论方法.

为　下文讨论的需要，我们先介绍如下一个与无限群有关的概念.

定义 5.2 设 $\{H_i \mid i \in I\}$ 为群的集合，B 为一群，$B_i \le H_i$，$B_i \cong B$. 设 α_i 为 B_i 到 B 的同构对应，$\forall i \in I$, G 说是 $\{H_i \mid i \in I\}$ 关于群 B 的 *自由融合积* (free amalgmated product)，若 G 同构于由全体 $H_i, i \in I$ 所生成的自由积 H 模由 H 中所有形状为 $b_i^{-1}(b_i^{\alpha_i\alpha_j^{-1}})$, $b_i \in H_i$, 的元素所生成的正规子群的商群，其中 i 遍历 I, 且 $i, j \in I$ 为各种可能的下标对. 群 G 也说是 $\{H_i \mid i \in I\}$ 关于群 B 的 *融合*.

由于我们主要兴趣在于考虑融合理论在有限群论中的应用，因此，我们常以以下比较特殊的方式定义秩 2 抛物系.

定义 5.3 令 G 为一群，P_1, P_2, 为 G 的有限子群，$B = P_1 \cap P_2$. 我们把三元组 $(G; P_1, P_2)$ (或四元组 $(G; P_1, P_2; B)$) 叫做一个秩 2 特征 p 抛物系或叫做一个秩 2 特征 p 融合，若以下条件成立：

(1) $G = \langle P_1, P_2 \rangle$;

(2) B 中不包含 G 的非平凡正规子群;

(3) $O_p(P_i) \neq 1, i = 1, 2$;

(4) $C_{P_i}(O_p(P_i)) \leq O_p(P_i), i = 1, 2$;

(5) $\mathrm{Syl}_p(B) \subseteq \mathrm{Syl}_p(P_1) \cap \mathrm{Syl}_p(P_2)$.

为了解决秩 2 抛物系问题, 我们通常采用下述的陪集图 (coset graph) 方法.

定义 5.4 设 G 为一群, P_1 和 P_2 为 G 的子群, $G = \langle P_1, P_2 \rangle$. 令 $\Gamma = \Gamma(G; P_1, P_2) = \{P_i x \mid i = 1, 2; x \in G\}$. $P_i x$ 称为 Γ 的顶点; 若 $P_i x \neq P_j y$ 且 $P_i x \cap P_j y \neq \varnothing$, 则说 $P_i x$ 和 $P_j y$ 是邻接的. Γ 对这样规定的邻接关系构成一个图, 叫做 G 关于 P_1, P_2 的陪集图. G 通过右乘作用在 Γ 上.

注意, 若 $(G; P_1, P_2)$ 为一秩 2 抛物系, 对于确定且有限的 P_1, P_2, G 并非确定的, 甚至也未必是有限的. 若 $B = P_1 \cap P_2$, 则 $(P_1, P_2; B)$ 所生成的最大的完备是融合积 $P_1 *_B P_2$, 其它的完备都是该融合积的同态像. Serre 证明了, 对于给定的 $(G; P_1, P_2; B)$, $\Gamma(G; P_1, P_2; B)$ 为一树. Serre 的结果对于利用陪集图解决秩 2 抛物系问题带来了很大方便. 因此秩 2 抛物系通常也叫做秩 2 融合.

令 Γ 为定义 5.4 中所定义的陪集图. 我们以小写字母 $\alpha, \beta, \cdots$ 表示 Γ 的顶点, $\Delta(\alpha)$ 表示 Γ 中与 α 相邻接的顶点之集合. Γ 中一条长为 n 的道路为一 $n+1$ 元序组 $(\alpha_0, a_1, \cdots, \alpha_n)$, 其中 $\alpha_i \in \Gamma$, 且对于 $0 \leq i, j \leq n$, $i \neq j$, 成立:

(i) $\alpha_i \neq \alpha_j$, 其中 $\{i, j\} \neq \{0, n\}$ 及

(ii) α_i 与 α_{i+1} 邻接.

两个顶点 δ 和 λ 说是共轭的, 若有 $g \in G$ 使 $\delta^g = \lambda$. 我们以 $d(\delta, \lambda)$ 表示两个顶点间的距离.

下面是陪集图 Γ 的一些基本性质.

命题 5.5 令 $(G; P_1, P_2)$ 为一秩 2 融合, Γ 为 G 关于 P_1, P_2 的陪集图. 则

(1) Γ 为 2-可分且连通的;

(2) $G \leq \mathrm{Aut}(\Gamma)$;

(3) G 在 Γ 上的作用为边传递而非顶点传递的;

(4) 设 $P_i x = \delta \in \Gamma$, 则 $|\Delta(\delta)| = |P_i : B|$, 且 G_δ 在 $\Delta(\delta)$ 上传递;

(5) $\forall \delta \in \Gamma$, G_δ 在 G 中与 P_1 或 P_2 共轭;

(6) Γ 中的边 (α, β) 的稳定子 $G_{\alpha\beta}$ 在 G 中与 B 共轭.

命题 5.5 中所有结论均可直接由定义得出.

下列命题是绝大多数有关秩 2 抛物系的问题所必不可少的.

命题 5.6 令 $\Gamma = \Gamma(G; P_1, P_2)$. 设 $\alpha, \beta \in \Gamma$ 且 $\beta \in \Delta(\alpha)$, 并假定 $U \leq G_\alpha \cap G_\beta$. 令 $X = N_G(U)$, 假定 $\forall \delta \in \{\alpha, \beta\}$, X_δ 在 $\Delta(\delta)$ 上传递, 则 $U = 1$.

证　令 $\Gamma_0 = \alpha^X \cup \beta^X$. $\forall x \in X$, $u \in U$, $(\alpha^x)^u = \alpha^{(xux^{-1})x} = \alpha^x$. 这表明, U 平凡作用在集合 α^X 上. 类似地可证 U 平凡作用在 β^X 上, 从而 U 平凡作用在 Γ_0 上. 由于 X 分别在 α^X 上和 β^X 上传递, 故 $\forall \lambda \in \Gamma_0$, $\Delta(\lambda) \subseteq \Gamma_0$. 这意味着 $\Gamma_0 = \Gamma$. 从而由命题 5.5(2), 即得 $U = 1$. □

我们将通过一个例子向读者介绍解决抛物系问题的一种行之有效的方法. 在进一步讨论之前, 我们先固定一些符号, 并证明几个基本性质.

设 (G, P_1, P_2) 为一秩 2 融合, $\Gamma = \Gamma(G; P_1, P_2)$ 为其陪集图. 对于 $\delta \in \Gamma$, 记

$$\begin{aligned}
Q_\delta &= O_p(G_\delta), \\
Z_\delta &= \langle \Omega_1(Z(T)) \mid T \in \mathrm{Syl}_p(G_\delta) \rangle, \\
V_\delta &= \langle Z_\lambda \mid \lambda \in \Delta(\delta) \rangle, \\
b_\delta &= \min\{d(\delta, \lambda) \mid Z_\delta \not\subseteq Q_\lambda \rangle, \\
b &= \min\{b_\delta \mid \delta \in \Gamma\}.
\end{aligned}$$

易知我们可找到 $\alpha \in \Gamma$, 使 $b_\alpha = b$. 这时可找到 α' 使 $d(\alpha, \alpha') = b_\alpha = b$ 且 $Z_\alpha \not\leq Q_{\alpha'}$. 这时 (α, α') 说是一对临界偶.

假定 $\gamma = (\alpha, \beta, \cdots, \alpha')$ 为由 α 到 α' 且长为 b 的路, 则 γ 可改写为 $\gamma = (\alpha, \alpha+1, \cdots, \alpha+b)$ 或 $\gamma = (\alpha'-b, \alpha'-b+1, \cdots, \alpha')$.

D. Goldschmidt 在文章 "Automorphisms of trivalent graphs, *Ann.of Math.*, **111**(1980), 377–406" 中首先提出了陪集图方法. B. Stellmacher 对他的方法加以改进, 建立了 (Z_α, b_α) 方法, 取得了不少令人瞩目的结果. 当前这种方法被认为是有限单群分类定理证明的基本方法之一.

下列命题给出了陪集图一些基本的群论性质.

命题 5.7 令 $\Gamma = (G; P_1, P_2)$ 为 G 关于 P_1 和 P_2 的陪集图, 则 $\forall \delta \in \Gamma$, 成立

(1) $Q_\delta = (\bigcap_{\lambda \in \Delta(\delta)} G_\lambda) \cap G_\delta$;

(2) $\forall \delta \in \Gamma$, Z_δ char G_δ, V_δ char G_δ, Q_δ char G_δ;

(3) $\forall \lambda \in \Delta(\delta)$, $Q_\delta Q_\lambda \trianglelefteq G_\delta \cap G_\lambda$;

(4) $Z_\delta \leq Q_\delta$, 即 $b_\delta \geq 1$, 特别地 $b \geq 1$. 又成立 $C_{G_\delta}(Z_\delta) = Q_\delta$ 或 $Z_\delta = \Omega_1(Z_\delta)$, 特别地, Z_δ 为初等可换群.

(5) 若 $Z_\delta \leq Z(T_\delta)$, $T_\delta \in \mathrm{Syl}_p(G_\delta)$, 则 $Z_\delta = \Omega_1(Z(G_\delta))$.

(6) 若 $\lambda \in \Delta(\delta)$, $Z_\lambda = \Omega_1(Z(G_\lambda))$, 则 $Z(G_\delta) = 1$.

由 Z_α 的定义和命题 5.7 可知, 利用 (Z_α, b_α) 陪集图考察秩 2 融合时, 应当区分以下两种情况: $[Z_\alpha, Z_{\alpha'}] = 1$ 和 $[Z_\alpha, Z_{\alpha'}] \neq 1$. 由以下两个命题, 我们可以更清楚地看到这种区分是必要的.

命题 5.8 假定 $[Z_\alpha, Z_{\alpha'}] \neq 1$, 则

(1) $[Z_\alpha, Z_{\alpha'}, Z_{\alpha'}] = [Z_{\alpha'}, Z_\alpha, Z_\alpha] = 1$;

(2) $b_\alpha = b_{\alpha'}$.

命题 5.9 假定 $[Z_\alpha, Z_{\alpha'}] = 1$, 则

(1) $b_{\alpha'} < b_\alpha \equiv 1 (\mathrm{mod}\ 2)$, 特别地, α 和 α' 不互相共轭;

(2) $[V_\beta, V_{\alpha'}, V_{\alpha'}] = [V_{\alpha'}, V_\beta, V_\beta] = 1$.

下面我们证明 Goldschmidt 的三度图的自同构群定理中的一种情况.

命题 5.10 (1) $G_2(2)' = PSU(3,3)$ 中具有秩 2 抛物系 (P_1^*, P_2^*), 其中 $P_1^* \cong (Q_8 * Z_4)S_3$, $P_2^* \cong (Z_4 \times Z_4)S_3$.

(2) $G_2(2)$ 中具有秩 2 抛物系 (P_1^*, P_2^*), 其中 $P_1^* \cong (Q_8 * Q_8)S_3$, $P_2^* \cong (Z_4 \times Z_4)D_{12}$.

(注意以上 $Q_8 * Z_4$ 和 $Q_8 * Q_8$ 分别表示 Q_8 与 Z_4 和 Q_8 与 Q_8 的中心积. 这两个中心积的中心都同构于 Z_2.)

定理 5.11 设 $(G; P_1, P_2)$ 为一秩 2 融合, 其中 $P_1/O_2(P_1) \cong S_3, P_2/O_2(P_2) \cong S_3$. 我们构造陪集图 $\Gamma(G; P_1, P_2)$, 并采用 (5.1) 中的符号. 假定 $[Z_\alpha, Z_{\alpha'}] \neq 1$, 且 α 和 α' 共轭. 则 G 相似于 $U_3(3)$ 或 $G_2(2)$, 即有, $O_2(P_1) \cong Q_8 * Z_4$, $O_2(P_2) \cong Z_4 \times Z_4$; 或 $O_2(P_1) \cong Q_8 * Q_8$, $O_2(P_2) \cong (Z_4 \times Z_4)Z_2$.

在给出定理 5.11 的证明之前, 我们先证明两个引理.

引理 5.12 假定 $\Gamma(G; P_1, P_2)$ 为定理 5.11 中所定义的陪集图, 则对于 $\lambda \in \Delta(\delta)$, 若 $W \leq Q_\delta, W \not\leq Q_\lambda$, 则成立

(i) $WQ_\lambda = Q_\delta Q_\lambda \in \mathrm{Syl}_2(G_\delta \cap G_\lambda)$.

(ii) 设 $\mu \in \Delta(\delta)$, 若 $U \leq Q_\mu, U \not\leq Q_\delta Q_\lambda$, 则 $\langle U, W\rangle Q_\lambda = G_\lambda$, 特别地 $\exists g \in G_\lambda$ 使 $\langle W, W^g\rangle Q_\lambda = G_\lambda$.

证 由定理 5.11 中假定条件即可得 (i),(ii). □

引理 5.13 $b = b_\alpha = 2$.

证 设 $\alpha \in \Gamma$, 能使 $b = b_\alpha$, 且 $(\alpha, \beta, \alpha+2, \cdots, \alpha')$ 为连接 α 和 α' 的道路. 由假定, α 与 α' 共轭, 故由命题 5.5(1), $b = b_\alpha \equiv 0 (\mathrm{mod}\ 2)$. 由 $[Z_\alpha, Z_{\alpha'}] \neq 1$ 可知 $Z_{\alpha'} \not\leq Q_\alpha$, 故成立 $Z_{\alpha'}Q_\alpha = Q_\beta Q_\alpha = S \in \mathrm{Syl}_2(G_\alpha)$.

(1) 可以找到 $\alpha \in \Gamma$, 使 $b = b_\alpha$ 且 $Z_\beta = \Omega_1(Z(G_\alpha)), \forall \beta \in \Delta(\alpha)$.

假定相反, 则由命题 5.7(4), $C_{G_\beta}(Z_\beta) = Q_\beta$. 记 $R = [Z_\alpha, Z_{\alpha'}]$, 则 $R \leq Z_\alpha \cap Z_{\alpha'}$. 若有 $\alpha - 1 \in \Delta(\alpha)$ 能使 $Z_{\alpha-1} \leq Q_{\alpha'-1}$, 则

$[Z_{\alpha-1}Z_\alpha, Z_{\alpha'}] = R \le Z_{\alpha-1}Z_\alpha$. 由此可知 $Z_{\alpha-1}Z_\alpha \trianglelefteq \langle Q_{\alpha-1}, Z_{\alpha'}\rangle = G_\alpha$. 故有 $Q_{\alpha-1} \cap Q_\alpha = C_{G_\alpha}(Z_{\alpha-1}Z_\alpha) \trianglelefteq G_\alpha$, 这就迫使 $Z_{\alpha-1} \le Z(Q_\alpha Q_{\alpha-1})$. 由命题 5.7(5) 可知 $Z_{\alpha-1} = \Omega_1(Z(G_{\alpha-1}))$. 由此立知 $Z_\beta = \Omega_1(Z(G_\beta))$, $\forall \beta \in \Delta(\alpha)$. 现假定有 $\alpha - 1 \in \Delta(\alpha)$ 使 $Z_{\alpha-1} \not\le Q_{\alpha'-1}$. 这时若存在 $\alpha-2 \in \Delta(\alpha-1)\setminus\{\alpha\}$, 使 $Z_{\alpha-2} \not\le Q_{\alpha'-1}$, 则由以上结果立得 $[R, G_{\alpha'-2}] = 1$, 这就迫使 $R = 1$, 矛盾. 若 $Z_{\alpha-2} \le Q_{\alpha'-2}$, 则可如前证明 $Z_{\alpha-2} = \Omega_1(Z(G_{\alpha-2}))$. 由于 $\alpha-2$ 与 α 共轭, 立得矛盾.

(2) $Z_\alpha \cong Z_2 \times Z_2$, $R = Z_\beta \cong Z_2$, $Z_\alpha = Z_\beta Z_{\alpha-1}$, $[Q_\beta, V_\beta] = Z_\beta$.

我们有 $2 = |Z_\alpha Q_{\alpha'}/Q_{\alpha'}| = |Z_\alpha / Z_\alpha \cap Q_{\alpha'}| = |Z_\alpha / C_{Z_\alpha}(Z_{\alpha'})|$. 易知 $C_{Z_\alpha}(\langle Z_{\alpha'}, Z_{\alpha'}^g\rangle) \le \Omega_1(Z(G_\alpha))$. 故有 $|Z_\alpha| \le 4$. 由于 Z_α 为 G_α 非平凡模, 故成立 $Z_\alpha \cong Z_2 \times Z_2$. 其余结论是显然的.

(3) 若 $b > 2$, 则 $b > 6$.

设 $2 < b \le 6$, 则有 $b = 4$ 或 $b = 6$. 若 $b = 4$, 则由 (2) 得 $R = [Z_\alpha, Z_{\alpha'}] = Z_\beta = Z_{a'-1} = Z_{\alpha+3}$. 由此得 $Z_{\alpha+2} = Z_\beta Z_{\alpha+3} = Z_\beta$, 这是不可能的. 类似地可证 $b \ne 6$.

(4) $b = 2$.

假定 $b > 2$, 则由 (3), 有 $b > 6$. 现考虑 $V_{\alpha-1}$ 的作用. 若 $V_{\alpha-1} \not\le Q_{\alpha'-2}$, 则有 $[Z_{\alpha'-1}, G_{\alpha'-2}] = [R, \langle V_{\alpha-1}, Q_{\alpha'-1}\rangle] = 1$, 矛盾. 故假定 $V_{\alpha-1} \le Q_{\alpha'-2}$. 若 $V_{\alpha-1} \le Q_{\alpha'-1}$, 则可如 (1) 之证明过程得出矛盾. 最后我们考察如下情况: $V_{\alpha-1} \le Q_{\alpha'-2}, V_{\alpha-1} \not\le Q_{\alpha'-1}$.

假定有 $\delta \in \Gamma$, $d(\alpha, \delta) = 4$ 能使 $Z_\delta \not\le Q_{\alpha'-4}$. 由于 $R = Z_{\alpha'-1}$, 故有 $[Z_{\alpha'-1}, Z_\delta] = 1$. 易知 $Z_{\alpha'-4}Z_{\alpha'-2} = Z_{\alpha'-4}Z_{\alpha'-1}$. 故有 $Z_{\alpha'-4}Z_{\alpha'-2} \triangleleft \langle Z_\delta, Q_{\alpha'-3}\rangle = G_{\alpha'-4}$. 显然 $G_{\alpha'-4} \cap G_{\alpha'-3}$ 不固定 $\alpha' - 2$. 又 $|\Delta(\alpha'-3)| = 3$, 故 $G_{\alpha'-4} \cap G_{\alpha'-3}$ 在 $\Delta(\alpha'-3) \setminus \{\alpha'-4\}$ 上传递, 从而有 $V_{\alpha'-3} \le Z_{\alpha'-4}Z_{\alpha'-2}$. 又由 $V_{\alpha'-3}$ 之定义可知 $V_{\alpha'-3} = Z_{\alpha'-4}Z_{\alpha'-2}$, 矛盾.

令 $W_\alpha = \langle Z_\lambda \mid d(\lambda, \alpha) \le 2\rangle$, $T_{\alpha-1} = \langle Z_\delta \mid d(\delta, \alpha-1) \le 3\rangle$. 以上讨论表明 $T_{\alpha-1} \le Q_{\alpha'-4}$. 由于 $[T_{\alpha-1}, Z_{\alpha'-1}] = [T_{\alpha-1}, R] = 1$, 故 $T_{\alpha-1} \not\le Q_{\alpha'-3}$, $T_\alpha \not\le Q_{\alpha'-2}$ 均不成立. 这表明 $T_{\alpha-1} \le Q_{\alpha'-2}$. 由此可得 $[T_{\alpha-1}, V_{\alpha'-1}] = [V_{\alpha-1}, V_{\alpha'-1}] = [W_\alpha, W_{\alpha'-1}] \le W_\alpha \le T_{\alpha-1}$.

从而有 $T_{\alpha-1} \lhd \langle Q_{\alpha-1}, V_{\alpha'-1}\rangle = G_\alpha$, 矛盾. 这就证明了 $b = b_\alpha = 2$. □

定理 5.11 的证明 由引理 5.12, $b = b_\alpha = 2$ 且 $Z_\alpha \cong Z_2 \times Z_2$, $Z_\beta = \Omega_1(Z(G_\beta))$. 记 $D_\alpha = (\bigcap_{\delta\in\Delta(\alpha)} Q_\delta) \cap Q_\alpha$.

(1) $[D_\alpha, G_\alpha] = Z_\alpha$.

显然 $Z_\alpha \le D_\alpha$. 又 $[D_\alpha, Z_{\alpha'}] = [Z_\alpha, Z_{\alpha'}] \le Z_\alpha$, 从而由 $D_\alpha \trianglelefteq G_\alpha$, 可立得结论.

(2) D_α 为初等可换群.

由于 $D_\alpha \le Q_\beta$, 故有 $\Phi(D_\alpha) \le \Phi(Q_\beta) \le Q_{\alpha'}$. 由此得 $[\Phi(D_\alpha), \langle Z_{\alpha'}, Z_{\alpha'}^g\rangle] = 1$. 若 $\Phi(D_\alpha) \ne 1$, 则因 $\Phi(D_\alpha) \trianglelefteq Q_\alpha$, 即得 $Z(G_\alpha) \ge \Phi(D_\alpha) \cap Z(Q_\alpha) \ne 1$, 矛盾.

(3) $Q_\alpha/D_\alpha \cong Z_2 \times Z_2$.

为此仅需证 $D_\alpha = Q_\beta \cap Q_{\alpha-1}$. 我们有 $[Q_\beta \cap Q_{\alpha-1}, Z_{\alpha'}] \le [Q_\beta, Z_{\alpha'}] = R \le Q_\beta \cap Q_{\alpha-1}$. 这表明 $Q_\beta \cap Q_{\alpha-1} \trianglelefteq \langle Z_{\alpha'}, Z_{\alpha'}^g\rangle Q_\alpha = G_\alpha$, 其中 $g \in G_\alpha$ 且 $\beta^g = \alpha - 1$. 故有 $D_\alpha = Q_\beta \cap Q_{\alpha-1}$.

(4) V_β/Z_β 为初等可换群.

由于 $[Z_\lambda, Z_\delta] \le Z_\beta$, $\forall \lambda, \delta \in \Delta(\beta)$, 立得结论.

(5) $|D_\alpha| \le 2^3$.

记 $U = \langle Z_{\alpha'}, Z_{\alpha'}^g\rangle$, 则 $UQ_\alpha = G_\alpha$. 取 $d \in U$, $o(d) = 3$. 由 V_β 的定义可知, $|V_\beta| \le 2^4$. 若 $|V_\beta| = 2^3$, 则由于 V_β 中包含不止一个 2 阶元, 故 $V_\beta \cong D_8$. 由于 $\mathrm{Aut}(D_8) \cong D_8$, 故 d 平凡作用在 V_β 上, 矛盾. 故必有 $|V_\beta| = 2^4$.

记 $\overline{V}_\beta = V_\beta/Z_\beta$, 则 d 作用在 $\overline{V}_\beta$ 上, $[\overline{V}_\beta, d] \cong Z_2 \times Z_2$. $[\overline{V}_\beta, d]$ 在 V_β 中的原像 H_β 必同构于 Q_8. 由于 D_α 为初等可换群, 故 $V_\beta \cap Q_\alpha \not\le D_\alpha$. 由 U 之定义可知 $D_\alpha = C_{D_\alpha}(U) \times Z_\alpha$. 记 $D_0 = C_{D_\alpha}(U)$. 令 $x \in Q_\alpha \cap V_\beta \setminus D_\alpha$, 则 $C_{D_0}(U)$ 被 $D_\alpha[\langle x\rangle, \langle d\rangle] = Q_\alpha$ 中心化, 这就迫使 $C_{D_0}(x) = 1$. 另一方面, $[D_\alpha, x] \le Z_\beta$. 由于 $|Z_\beta| = 2$, $x^2 \in D_\alpha$, 故 $|D_0| = |D_0 : C_{D_0}(x)| \le 2$, 从而成立 $|D_\alpha| \le 2^3$.

至此, 我们已不难确定 $O_2(P_1)$ 和 $O_2(P_2)$ 的结构. 若 $|D_\alpha| = 2^3$, 则有 $O_2(P_1) \cong Q_\alpha \cong Q_8 * Q_8$, $O_2(P_2) \cong Q_\beta \cong (Z_4 \times Z_4)Z_2$; 若

$|D_\alpha| = 2^2$, 则有 $O_2(P_1) \cong Q_\alpha \cong Q_8 * Z_4$, $O_2(P_2) \cong Q_\beta \cong Z_4 \times Z_4$.

请读者自行完成有关证明. □

由定理 5.11 可知, 参数 $b = b_\alpha$ 与 Q_α, Q_β 的结构有着密切关系, 在许多情况下, $b = b_\alpha$ 等于 Q_α 或 Q_β 中非中心主因子的个数.

子群 Z_α 的定义方式十分值得注意. 首先, Z_α 是初等可换的, $Z_\alpha \le Q_\alpha$. 实际上, 许多情况下 $Z_\alpha = \Omega_1(Z(Q_\alpha))$. 但 Z_α 比 $\Omega_1(Z(Q_\alpha))$ 具有更好的性质: $C_{G_\alpha}(Z_\alpha) = Q_\alpha$ 或 $Z_\alpha = \Omega_1(Z(G_\alpha))$. 又由命题 5.8 可知, 当 $[Z_\alpha, Z_{\alpha'}] \ne 1$ 时, 成立 $[Z_{\alpha'}, Z_\alpha, Z_\alpha] = 1$, 即 Z_α 在 $Z_{\alpha'}$ 上是所谓二次作用的. (p-群 A 说是在 $GF(p^n)$-模 V 上二次作用, 若 $[V, A, A] = 1$). 这样就为我们限制商群对的范围, 提供了一定的条件. 最后, 通常 Z_α 是 G_α 的不可约模, 并且它的结构比较容易确定. 这就为我们确定 Q_α 的结构, 提供了一个很好的出发点.

融合理论与有限单群理论有着密切关系. 在下一节, 我们还将介绍融合方法对于有限单群分类的作用.

§6. 有限单群简介

1980 年 2 月, 有限单群分类定理宣告"成立". 这是 20 世纪数学领域最伟大的成就之一. 自 50 年代初至 1980 年, 先后有数以百计的数学工作者参与了这一定理的证明工作. 应当说分类定理是一个研究领域, 它的结果以及为证明这一定理而发展起来的一系列方法对于代数学及其它诸多数学分支的发展都将产生深远的影响. 本节中我们简单介绍这方面的情况. 有兴趣的读者可参阅下列文献:

D.Gorenstein, Classifying finite simple gourps, *Bull. Amer. Math. Soc.*, Vol.14, No.1–2 (1986), 1–98.

R.Solomon, On finite simple groups and their classification, *Notices Amer. Math. Soc.*, Vol.42, No. 2 (1995), 231–239.

§6.1 有限单群简介

最早发现的单群是 A_5, 它是伽罗瓦于 19 世纪 20 年代末发现的. 最后发现的一个单群是 J_4, 它是 J. Janko 于 1976 年发现的. 有限单群包括以下四类:

(1) 素数阶循环群;

(2) 交错群 $A_n(n \geq 5)$;

(3) 16 个 Lie 型群系列;

(4) 26 个零散单群.

(1), (2) 两类是大家早已熟知的, 下面我们分别介绍最后两类. Lie 型群包括 16 个群系列. 表 6.1 给出了所有的 Lie 型群系列和它们的阶.

Lie 型群族中包含我们在第 XI 章中考察过的典型群族. Dickson 于 1901 年考察了有限域上典型群. 到了 50 年代, Chevalley 注意到类似于复单 Lie 群的情况, 通过考察上单 Lie 代数的自同构群, 可以定义表 6.1 中前八个单群系列; 稍后, Tits, Steinberg, Suzuki 和 Ree 等人又利用适当的域自同构和图自同构构造了后面八个扭群族.

值得注意的是 Lie 型群具有多种相当一致的定义方法: 某些 Lie 代数的自同构群及这些群的固定点; 半单 Lie 代数群的某些自同态的固定点; 有限秩厦的自同构群; 有限秩 BN-对的自同构群等等.

零散单群 是指那些既不是交错群又非 Lie 型群的非可换单群. 早在 19 世纪 60 和 70 年代, 就发现了五个零散单群. 一个世纪之后, 在 1965 到 1974 的 10 年间, 才又陆续发现了其余的 21 个零散单群. 为了使读者对零散单群有比较完整的印象, 我们列出以下表 6.2.

表 6.1: Lie 型单群表

群名称	阶	备注
$A_n(q)$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-1)$	$PSL(n,q)$
$B_n(q)$ $n>1$	$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$	$P\Omega(2n+1,q)$ q 为奇数
$C_n(q)$ $n>2$	$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$	$PSp(2n,q)$
$D_n(q)$ $n>3$	$q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$	$P\Omega_{+1}(2n,q)$
$G_2(q)$	$q^6(q^6-1)(q^2-1)$	
$F_4(q)$	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	
$E_6(q)$	$q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)$ $\cdot(q^5-1)(q^2-1)$	
$E_7(q)$	$q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)$ $\cdot(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$	
$E_8(q)$	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)$ $\cdot(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$	
${}^2A_n(q)$ $n>1$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-(-1)^{i+1})$	$PU(n,q)$
${}^2B_2(q)$ $q=2^{2m+1}$	$q^2(q^2+1)(q-1)$	Ree-Suzuki
${}^2D_n(q)$ $n>3$	$q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1)$	$P\Omega_{-1}(2n,q)$
${}^3D_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	Steinberg
${}^2E_6(q)$	$q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)$ $\cdot(q^5+1)(q^2-1)$	Steinberg
${}^2F_4(q)$ $q=2^{2m+1}$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	Ree
${}^2G_2(q)$ $q=3^{2m+1}$	$q^3(q^3+1)(q-1)$	Ree

在寻求新的单群过程中，有时新单群的发现者只是预言了新单群的存在及其性质，而把具体构造工作留给其他人或计算机去完成. 例如 1976 年， Janko 已经发现了零散单群 J_4，但直到 1980 年，诺顿 (Norton) 及其剑桥大学的同事才利用计算机证明了 J_4 的存在性，即给出了生成元的定义关系和唯一性. 在 1965 到 1974

表 6.2: 零散单群表

群	阶	发现者
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko
$J_2 =$ HJ	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Hall-Janko
$J_3 =$ HJM	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Higman-Janko-McKay
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31$ $\cdot 37 \cdot 43$	Janko
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman-Sims
Mc	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLauhlin
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki
Ly = LyS	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons-Sims
He = HHM	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held-Higman-McKay
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Rudvalis
O'N = O'NS	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	O'Nan-Sims
Co_3 =.3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_2 =.2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_1 =.1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway
M(22)$= F_{22}$	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Fischer
M(23)$= F_{23}$	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer
$M(24)' = F_{24}$	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$ $\cdot 23 \cdot 29$	Fischer
$F_3 = E$	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson
$F_5 = D$	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Harada
$F_2 = B$	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$ $\cdot 19 \cdot 23 \cdot 31 \cdot 47$	Fischer (Baby Monster)
$F_1 = M$	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17$ $\cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	Fischer-Griess (Monster)

年的十年间，为了寻求新的零散单群，并考察这些单群族新成员的性质，数学家们探索并构造了一些新的数学结构，甚至因而开辟了一些新的数学领域.

§6.2 有限单群分类定理要点

50 年代以来，在寻求新的单群的同时，群论学者们也在设法对有限单群进行分类. 经过 30 年的共同努力，终于获得了如下的分类定理.

有限单群分类定理：任何有限单群必然同构于上述四个群系中某个成员.

分类定理说明了这样一个事实：在同构意义下，所有有限单群均包含在上述四个群类之中. 特别地，不可能再构造“真正的”新单群. 证明分类定理的困难在于，我们定义单群时，往往是通过某种人为的外部条件，例如一组生成元定义关系，群在某一几何或组合结构上的作用，群在集合上的本原作用等等. 但单性却是群的内在性质. 因此要证明分类定理，必须从有限群的单性出发，证明所考察的群满足已知单群的某些给定条件. 由以上讨论可知，粗略地说，分类工作应当包含以下几个步骤：第一步，为所有已知单群找到适当的标记；证明带有某种特定标记的有限单群，必然同构于某个已知有限单群或某几个已知有限单群中的某一个. 第二步，证明任何有限单群必然具有以上所规定的某个标记或该标记的等价物.

1954 年，在 Amsterdam 世界数学家大会上 Brauer 提出了如下想法：设 G 为一非可换偶阶单群，选择 G 的一个对合 t. 证明 $C_G(t)$ 的同构型，确定了 G 的可能的同构型.

1962 年， Feit 和 Thompson 发表了著名的“奇阶定理”：任意奇阶群必然是可解群. 根据这一定理，任意单群中必然包含对合. 因此 $C_G(t)$ 是一种合适的标记.

选择 $C_G(t)$ 作为有限单群的标记，有一个很大的好处，由于 G 为单，所以 $C_G(t) < G$，从而我们可以采取一种归纳程序：假定 G 为一极小反例，即 G 为一单群，且不同构于任何已知单群，但 G 中任意单截段 Y/X，这里 $X \trianglelefteq Y \leq G$，必同构于某个已知单群. 这表明 $C_G(t)$ 可通过可解群或已知单群加以刻划.

按照这一设想，分类定理可以通过如下步骤完成：

(1) 证明任意非可换有限单群 G 中一定可以找到对合 t, 使 $C_G(t)$"相似于" 某个已知单群 G^* 中的对合 t^* 的中心化子 $C_{G^*}(t^*)$.

(2) 证明 $C_G(t)$ 与 $C_{G^*}(t^*)$ 相似将导致 $C_G(t) \cong C_{G^*}(t^*)$.

(3) 证明由 $C_G(t) \cong C_{G^*}(t^*)$, 可推知 $G \cong G^*$.

在分类工作进程中, 人们发现有时有必要考察奇阶元的中心化子. 人们还注意到考察群中某些 p-局部子群, 即 p-子群的正规化子, 更为方便. 这样就形成了分类工作中至关重要的一种方法—局部分析方法. 近年来, 局部子群的概念又推广为可解子群的正规化子.

在以上设想的基础上, Gorenstein 提出了他的有限单群分类纲领. 在此我们简单地介绍有关这一纲领的基本方面.

不难看出, 在上文分类的三个步骤中, 最困难也最重要的是第一个步骤.

为了以下行文方便, 我们先给出下述概念.

定义 6.1 设 G 为一群. 我们说 G 具有 p-秩 k, 若 G 中的极大初等交换 p-子群之阶为 p^k.

定义 6.2 设 G 为一群, t 为 G 中一个 p 阶元. 记 $H = C_G(t)$. 依第 V 章定义 4.9, H 的广义 Fitting 子群 $F^*(H) = F(H)M$, 其中 M 由式 $M/Z((F(H)) = \mathrm{Soc}(C_H(F(H))/Z(F(H)))$ 确定. 我们称 t 是半单的, 若 $M \neq 1$; 而称 t 是为*幂幺的*, 若 $F^*(H)$ 为一 p-群.

定义 6.3 称群 G 为*亚幂幺的*, 如果对 G 的所有满足 p-秩 ≥ 3 的素数 p 来说, G 的每个 p 阶元都是幂幺的.

以下我们假定 G 是单群, t 为 G 中对合, 即 2 阶元, $H = C_G(t)$. 为解决分类问题, 群论学者采取了下列步骤:

(i) 利用群的单性限制对合中心化子的结构.

通过考察已知单群, 人们注意到下列事实: 任何已知单群的对合的中心化子中 $2'$-可解正规子群必为单位群. 为了证明一个"未知的" 单群具有同样性质, 一个很自然的想法是考察 $O_{2'}(G)$

与 $O_{2'}(H)$ 间的关系. 人们期望得到如下结果: $O_{2'}(G)=1 \iff O_{2'}(H)=1$.

经过许多群论学者的共同努力, 对以上问题终于得到了肯定回答, 并且得到了以下结果.

定理 6.4 *若 G 为一 2-秩 ≥ 3 的单群, 则或者 G 中包含半单元, 或者 G 中所有 2 阶元均为幂幺的.*

(ii) 对所有 2-秩 ≥ 3 且包含半单元的单群进行分类.

Aschbacher 的分量定理为此提供了关键步骤. 据此, 人们证明了在这种情况下, H 必"相似于"某个已知单群中半单对合的中心化子.

(iii) 2-秩为 0 即奇数阶群的情况, 奇阶定理说不存在这样的非交换单群.

(iv) 2-秩等于 2 的有限单群的分类: 这由多位作者的一些长篇文章进行了完全分类.

(v) 亚幂幺群的分类, 又分为以下两种情况:

(a) 若有某个 2-局部子群的 p-秩 ≥ 3, p 为奇素数.

(b) 经典拟薄情况: 即对每个 2-局部子群, 其 p-秩均 ≤ 2, p 为奇素数. (若 p-秩均等于 1, 则说是薄的.)

迄今为止, 除步骤 (v)(b) 外, 其它情况的证明均已给出. 对于情况 (v)(b), Mason 长期从事这一情况的研究. 人们普遍认为这一情况是可以证明的. 但至今有关的证明尚未发表. 其原因在于, 一方面原有证明太长, Mason 完成的证明的预印本已长达 800 页以上; 另一方面, 由于近年来融合理论在有限单群理论中的成功应用, 特别是 Stellmacher 为薄群分类提供了一个简明的证明, 使 Mason 也有意于利用融合方法.

在拟薄情况下, 可以证明拟薄群 G 必然可由两个 2-局部子群 P_1 和 P_2 生成, P_1 和 P_2 包含 G 的共同的 Sylow 2-子群. 这样就可以利用融合方法. 采用这一方法最困难的步骤在于确定所有可能的群对 $(P_1/O_2(P_1), P_2/O_2(P_2))$. 在上一节的最后, 我们曾经指出, Z_α 的定义有助于限制上述群对的选择. 确定了群对

$(P_1/O_2(P_1), P_2/O_2(P_2))$, 融合方法将进一步发挥作用. 但还需指出, 利用融合方法确定 $O_2(P_1)$ 和 $O_2(P_2)$ 的结构之后, 证明由和已知单群的"相似性"过渡到和已知单群的同构, 仍是相当困难的工作, 但这已不足以影响整个的分类工作的进程了.

这一定理证明的完成大约还须若干时日, 但也为期不远了.

由以上介绍可以看出, 分类定理的证明极为复杂, 而且原有证明工作并非在一个统一的纲领之下进行的, 以致于多有重迭、交叉甚至错误. 因此自 80 年代中期起, Gorenstein 等人计划写出总数为十二部著作, 其中包括单群分类的系统完整的证明, 但至 Gorenstein 去世也未完成.

单群分类工作是 20 世纪数学史上的一个重要的里程碑. 这一工作的完成及分类工作进程中所产生的一系列方法对数学许多学科的发展都起到了推动作用.

(1) 分类定理本身为许多过去悬而未决的群论和其它数学学科中一些重大问题的解决提供了依据.

(2) 通过分类工作, 人们对有限单群的结构和性质有了比较系统深入的了解. 这就便于把有关单群的结果用于其它数学分支或群论的其它方向.

(3) 产生了一系列新的方法, 这些方法必可成为研究群论其它分支的行之有效的工具.

(4) 产生了一些新的颇具潜力的数学分支, 例如几何理论, 代数组合论等. 特别值得一提的是产生了一门"魔群学". 魔群指零散单群 F_1. 发现魔群后不久, 人们注意到 F_1 与经典椭圆函数间的奇妙关系. F_1 的特征标表与 Jacobi 模函数在 ∞ 处的展开系数十分吻合 (借助一些简单而自然的关系式). 为解释这一现象, 人们进一步注意到 F_1 同其它许多数学分支的密切关系, 吸引了不少研究者投入这方面的工作.

限于篇幅, 我们不再详细介绍更多的内容. 还需指出的是, 为了避免采用过多的术语和概念, 上文中个别概念的定义不完全规范. 有兴趣的读者可参看本节前面引述的文献.

习　题

1. 证明命题 1.5.

2. (1) 设 G 为一群， X, Y, Z 为 G 的子群. 证明下列条件等价:

(i) $(XY)\cap(XZ)=X(Y\cap Z)$;

(ii) $(X\cap Y)(X\cap Z)=X\cap(YZ)$;

(iii) 若陪集 aX, bY 和 cZ 两两有非空的交，则 $aX\cap bY\cap cZ\neq\varnothing$.

(2) 令 V, I 为集合 τ 为 V 到 I 的映射; 在 V 上定义了一个自反且对称的关系 $*$, $*$ 叫做 V 上的关联关系.

令

$$\mathcal{F}=\{A\subseteq V\mid A=\{x\mid x\in V, \text{ 且 } \forall x,y\in A, x*y\}\}.$$

证明 (i) 令 $\Delta=(V,\mathcal{F})$, 规定 $\subset$ 为 $\mathcal{F}$ 中元素间的包含关系，则 Δ 为一复形. 同构于 Δ 的复形称为旗复形;

(ii) 设 $\Delta=(V,\mathcal{F})$ 为一有限秩复形，则 Δ 为一旗复形当且仅当如下条件成立: 对于 V 中任意三元组 (x,y,z), 若该组中元素两两相互关联，则必有 $A\in\mathcal{F}$ 包含 x,y,z.

(iii) 命题 1.5 中所定义的复形 $\Delta(G;\mathcal{F})$ 为旗复形，当且仅当对于 $\mathcal{F}$ 中任意三个子群 G_i, G_j, G_k, (1) 中所列举的性质成立.

3. 证明定理 2.17.

4. (1) 令 (W,S) 为一 Coxeter 系. 对于 $s\in S$, 令 $P_s=\{w\in W\mid l(sw)>l(w)\}$. 证明

(i) 我们有 $\bigcap_{s\in S}P_s=1$;

(ii) 成立 $W=P_s\cup sP_s$ 及 $P_s\cap sP_s=\varnothing$;

(iii) 若 $w\in P_s$, 且 $ws'\notin P_s, s'\in S$, 则成立 $ws'=sw$.

(2) 令 W 为一群， S 为 W 中 2 阶元之集合， $W=\langle S\rangle$. 假定对于任意 $s\in S$, 都可以得到 W 的一个满足以下三个条件的子集 P_s:

(i) $1\in P_s$;

(ii) $sP_s\cap P_s=\varnothing$;

(iii) 若 $w\in P_s$ 且对于某个 $s'\in S$, $ws'\notin P_s$, 则成立 $ws'=sw$.

证明: (W,S) 为一 Coxeter 系，且有 $P_s=\{w\in W\mid l(sw)>l(w)\}$.

5. (1) 证明例 1.7 中所定义的复形为一厦.

(2) 设 G 为 $\Delta(\mathcal{P})$ 的自同构群，令 $G_C=B, G_\Sigma=N$. 证明:

(i) 如上定义的 B, N, 构成 G 中一个 BN-对.

(ii) 证明: 由例 4.2 可以得出 $PSL(n,q)$ 中的 BN-对, 且这样的 BN-对恰与以上所定义的 BN-对相一致.

6. 令 (G,B,N,S) 为一 Tits 系， $H\trianglelefteq G$. 证明若 $BH=P_J$, 其中 $J\subseteq S$, 则 J 和 $S\backslash J$ 间元素可换.

7. 设 $(G; P_1, P_2)$ 为一秩 2 融合，其中 $P_1/O_2(P_1) \cong S_3$, $P_2/O_2(P_2) \cong S_3$. 构造陪集图 $\Gamma(G; P_1, P_2)$ 并采用 (5.1) 的符号. 假定 $[Z_\alpha, Z_{\alpha'}] \neq 1$, 且 α 和 α' 不共轭. 则 $P_1 \cong P_2 \cong S_4$ 或 $P_1 \cong P_2 \cong S_4 \times Z_2$.

第 XIV 章

群与图

群和图一直都是人们研究得很多的数学对象．但是把二者结合起来，应用图来研究群以及应用群来研究图则是较近的事．R. Frucht 在 1938 年证明了对于任意给定的抽象群，都存在一个图以它为自同构群 (见 R. Frucht, Herstellung von Graphen mit vorgegebener abstrakten Gruppe, *Compositio Math.*, **6** (1938), 239–250), 这个重要的工作揭开了这个领域的帷幕．而 W.T. Tutte 的著名文章 "A family of cubical graphs," (载 *Proc. Cambr. Phil. Soc.*, **43** (1947), 459–474), 则可以看作是群对图论的第一个精彩的应用．但是，对这个领域的广泛的研究则是在 1960 年代以后．近三十年来，在这方面出现了很多重要的工作．例如，对于图论在群论上的应用，值得提出的是应用图论方法研究置换群，特别是研究本原群的次轨道结构．关于这方面我们已经在第 XII 章 §4 讲过，亦可见 P.M. Neumann 的精彩文章 "Finite permutation groups, edge-coloured graphs and matrices"(载 *Topics in Group Theory and Computation*, Acad. Press, 1977. pp.82–118.) 又，Higman-Sims 单群就是作为图的自同构群而发现的，它对于有限单群分类问题的完成做出了贡献．另一方面，应用群论于图论的研究在最近 30 年中则有着更丰富的结果，这是本章要着重介绍的．具体地说，本章的目的是把读者引入这第二个领域，介绍一些入门的知识以及这方面的一部分典型问题和方法．

我们不要求读者学过图论，因此在 §1–§2 中我们首先介绍图论的某些基本概念和术语. 在 §3 讲述图的自同构群，它是联系图与群的桥梁. 之后，则有选择地讲述具有较高对称性的图的理论，这类图的研究领域是群论最有用武之地的场所. 如在 §4 讲述的 Cayley 图，§5 的对称图，§6 的半传递图和半对称图等.

编写本章的主要参考书是 N. Biggs 的 *Algebraic Graph Theory*, (Cambr. Univ. Press, 1974) 和 N. Biggs 和 A.T. White 的 *Permutation Groups and Combinatorial Structures*, (Cambr. Univ. Press, 1979) 的第 4 章. 但也有一半或更多的内容无参考书可循，它们是第一次在书中出现的.

§1. 图的基本概念

我们所说的图，与几何中的图形和数学分析中的函数图象是不同的. 它实际上是带有某个特定的二元关系的有限集. 为了给出它的严格定义，我们先引进下面的

定义 1.1 设 V 是集合，称 V 的所有 *无序元偶* 的集合

$$V \cdot V = \{(u,v) \mid u,v \in V\}$$

为 V 和 V 的 *无序积*. (所谓 (u,v) 是无序元偶，即我们认为 $(u,v) = (v,u)$.) 记

$$V_0 = \{(v,v) \mid v \in V\},$$

则 $V^{\{2\}} = V \cdot V \setminus V_0$ 为 V 的所有二元子集的集合. 即

$$V^{\{2\}} = \{\{u,v\} \mid u,v \in V, u \neq v\}.$$

又，称 V 的所有 *有序元偶* 的集合

$$V \times V = \{(u,v) \mid u,v \in V\}$$

为 V 和 V 的 *笛卡儿积*. 仍记

$$V_0 = \{(v,v) \mid v \in V\},$$

则 $V^{(2)} = V \times V \setminus V_0$ 为 V 的所有二元不相同的有序元偶的集合.

为了方便起见， $V \cdot V$ 和 $V \times V$ 的元素有时都用圆括号表示，请读者注意区分.

下面我们在定义 1.2 和定义 1.3 中分别给出无向图和有向图的定义，无向图和有向图统称为图.

定义 1.2 称一对集合 V 和 E 为一个 无向图 X, 记作 $X = (V, E)$, 如果 V 是一个非空有限集 (V 的元素叫做图 X 的 顶点), 而 E 是 $V \cdot V$ 的一个子集 (E 的元素叫做图 X 的 边). 如果满足 $E \subseteq V^{\{2\}}$, 则称图 X 为 简单图.

我们以 $|X|$ 表 V 的势，即图 X 的顶点数；而以 $\|X\|$ 表 E 的势，即图 X 的边数. 对于一个图 X, 我们要求 V 必须是非空集合，但 E 可以是空集.

如果我们在一张纸上任意画出 $|X|$ 个点代表 X 的顶点集 $V(X) = \{v_1, \cdots, v_n\}$, 并且对于任一条边 $(v_i, v_j) \in E(X)$, 在点 v_i 和 v_j 间连一条线来代表，这就得到图 X 在平面上的一个 图示. 它可以使我们更直观地了解和把握这个图. 下面的图 1.1 就是图 X 和图 Y 的图示，它们的顶点集和边集分别是

$$\begin{aligned} V(X) &= \{v_1, v_2, v_3, v_4, v_5\}, \\ E(X) &= \{(v_1, v_3), (v_3, v_4), (v_4, v_5), (v_5, v_2), (v_2, v_4)\}; \end{aligned}$$

和

$$\begin{aligned} V(Y) &= \{a, b, c, d, e\}, \\ E(Y) &= \{(a, b), (a, e), (e, d), (e, e), (b, b)\}. \end{aligned}$$

图 Y 中的边 (b, b) 和 (e, e) 叫做 自环 (loop), 简单图不允许有自环. 因此，图 X 是简单图，但图 Y 不是.

注. 有些图论学者还允许 重边 (multi-edge), 即一条边可以在图中重复出现多次. 这种图叫做 重图 (multigraph), 它在我们的讨论中是不需要的. 实际上，在绝大多数场合，我们只讨论简单图，只在很少几个地方，才讨论有自环的图.

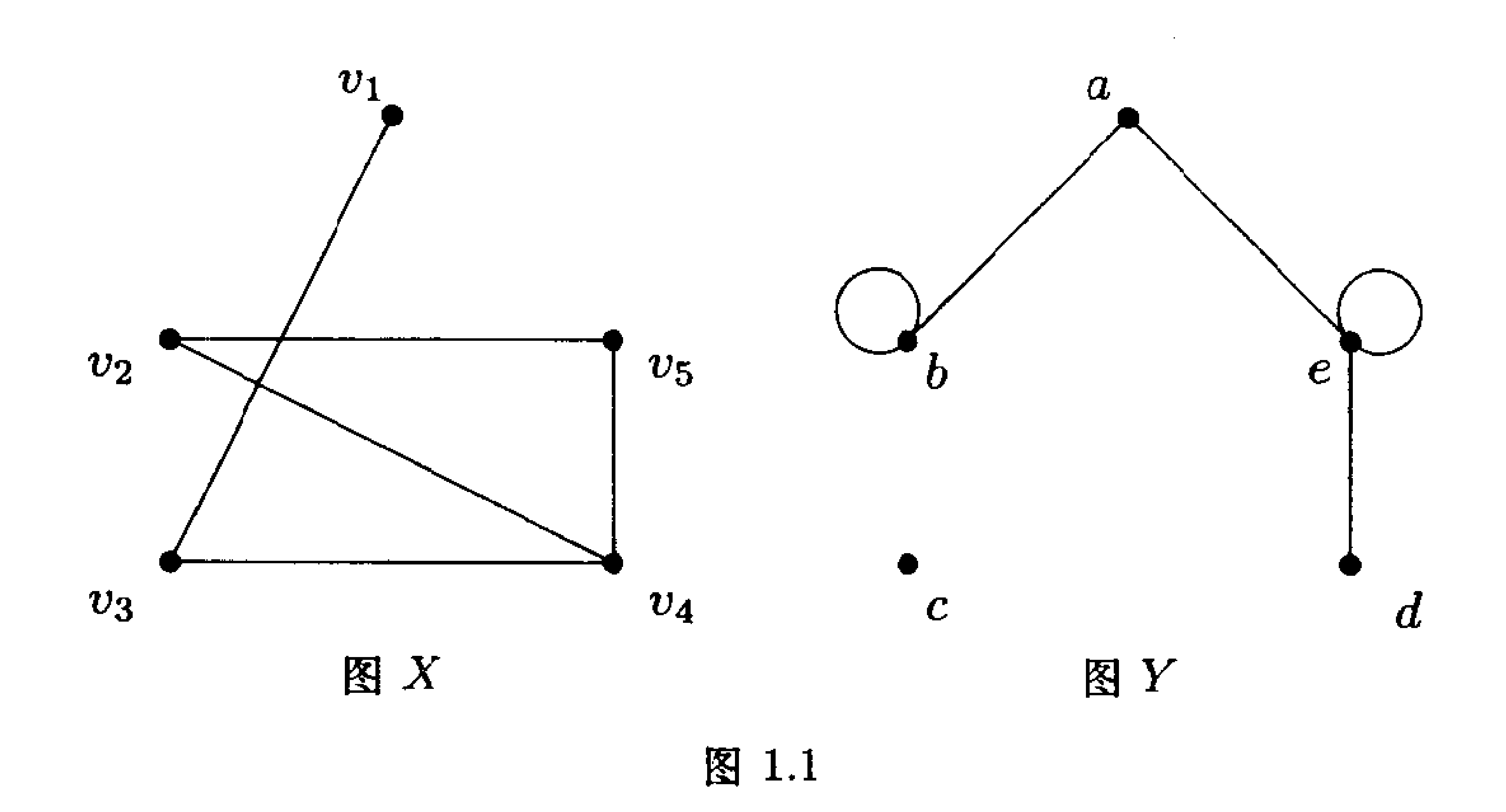


图 1.1

下面我们再给出有向图的定义，并对无向图和有向图的基本概念进行平行的叙述.

定义 1.3 称一对集合 V 和 E 为一个 *有向图* X，记作 $X = (V, E)$，如果 V 是一个非空有限集 (V 的元素叫做图 X 的顶点)，而 E 是 $V \times V$ 的一个子集 (E 的元素叫做图 X 的 *有向边* 或 *弧*). 如果满足 $E \subseteq V^{(2)}$，则称 X 为 *简单有向图*.

和无向图一样，我们也以 $|X|$ 表 V 的势，而以 $\|X\|$ 表 E 的势， E 也可以是空集.

有向图也有和无向图一样的图示，但要用箭头表明有向边的方向. 即如果 $(u, v) \in E$，则应在代表边 (u, v) 的线上标上由 u 到 v 的箭头，下面的图 1.2 是两个有向图 D_1 和 D_2 的图示，其中 D_1 是简单图， D_2 有自环，它不是简单图. 注意在图 D_1 中， (v_3, v_4) 和 (v_4, v_3) 是两条不同的 (有向) 边.

和无向图一样，有些图论学者在有向图中也允许重 (有向) 边，我们也不考虑这种更一般的图. 但要强调一点，上面图 D_1 中的边 (v_3, v_4) 和 (v_4, v_3) 可不是重边，它们是两条不同的边.

如果把有向图中各边的方向去掉，即认为它们是 $V \cdot V$ 的元素，那么就得到一个无向图，叫做该有向图的 *基础无向图*. 但应

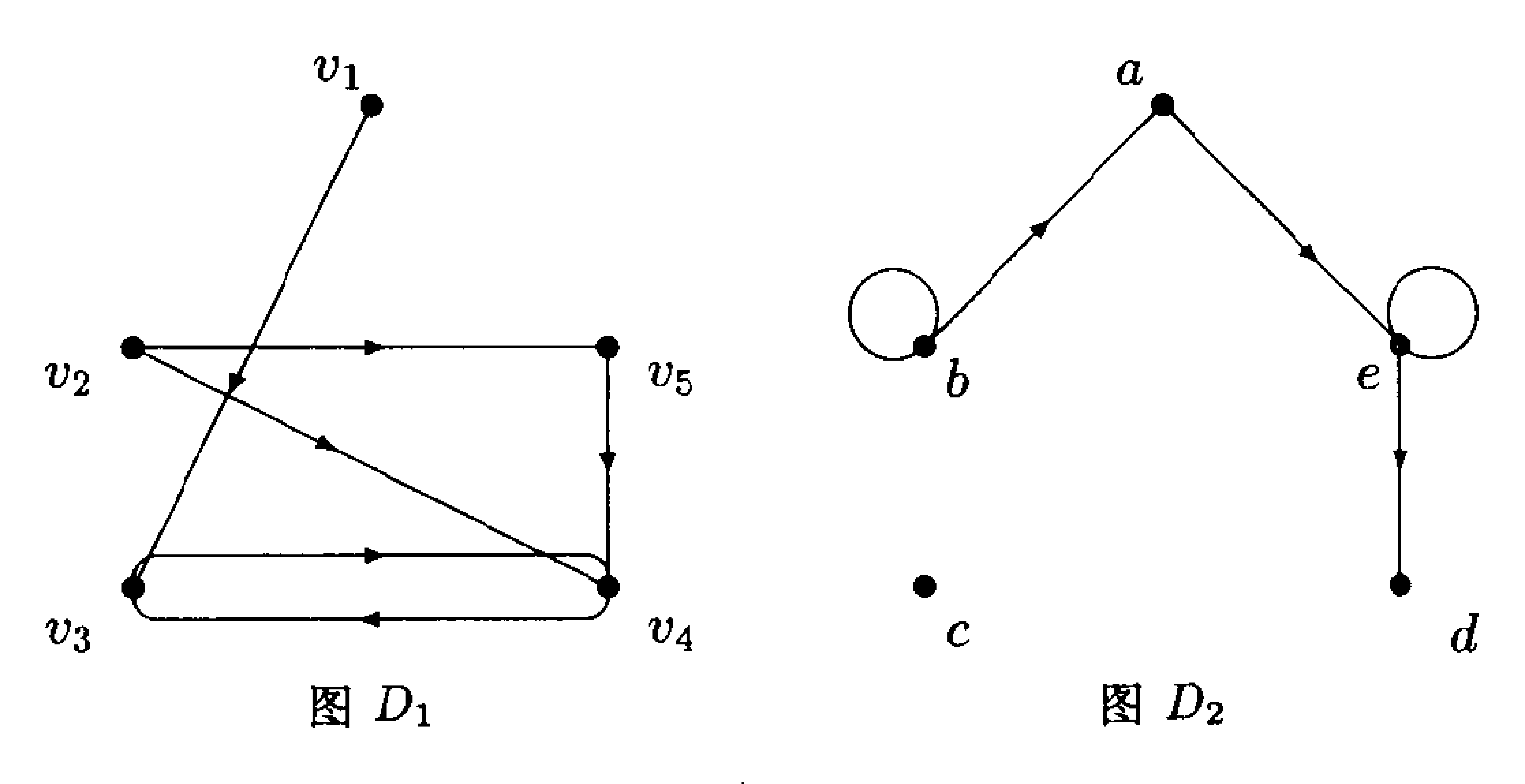


图 1.2

注意，如果 (u,v) 和 (v,u) 都是某有向图的边，去掉它们的方向，就得到相同的无向边. 由于我们不考虑重边，因此在它的基础无向图中只保留一个边 (u,v). 事实上，图 1.1 中的图 X (图 Y) 就是图 1.2 中的有向图 D_1 (图 D_2) 的基础无向图.

下面我们简要地叙述图论的一些最基本的概念.

设 $X=(V,E)$ 是一个 (有向或无向) 图，若 $e=(u,v)\in E$，即 (u,v) 是 X 的一条边，我们称顶点 u,v 为边 e 的 *端点*. 在有向图的情况，则进一步称 u 为边 e 的 *起点*, v 为边 e 的 *终点*, 并称边 e联结 点 u 和 v. 这时我们还称顶点 u 和 v 是 *相邻的*, 而 u(和 v) 与边 e 是 *相关的*.

对于无向简单图来说，顶点之间的相邻关系是最基本的关系，它实际上决定了这个图的结构. 为了更明确地表出这个关系，我们引进图的邻接矩阵的概念.

定义 1.4 设 $X=(V,E)$ 是一个 (有向或无向) 图，而 $V=\{v_1,v_2,\cdots,v_n\}$. 则称如下定义的 $n\times n$ 方阵 $\mathbf{A}=\mathbf{A}(X)$ 为图 X 的 *邻接矩阵*, 规定

$$a_{ij}=\begin{cases}1, & \text{如果}(v_i,v_j)\in E,\\ 0, & \text{如果}(v_i,v_j)\notin E.\end{cases}$$

例如, 图 1.1 中的图 X 和 Y 以及图 1.2 中的图 D_1 的邻接矩阵依次为

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array}\begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array}, \qquad \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array}\begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array},$$

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array}\begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}.$$

从中我们可以看出, 简单图的邻接矩阵的主对角线元素均为 0, 而无向图的邻接矩阵是对称的. 还应注意, 图的邻接矩阵并不是唯一确定的, 如果给图的顶点另外一个编号, 则邻接矩阵要发生变化, 请读者考虑一下将会怎样变化.

除了邻接矩阵之外, 由图的顶点和边的相关关系, 还可定义图的关联矩阵, 但它在我们这里并不需要, 有兴趣的读者可以参看一般的图论教科书.

由于顶点之间的相邻关系是图中的基本关系, 我们可以把图之间的 同构 定义为保持相邻关系的顶点集之间的一一映射.

定义 1.5 设 $X = (V,E)$ 和 $X' = (V',E')$ 是两个 (有向或无向) 图, φ 是 V 到 V' 上的一一映射, 满足对于所有的 $u,v \in V$,

$$(u,v) \in E \iff (u^\varphi, v^\varphi) \in E',$$

则称 φ 为图 X 到图 X' 上的同构映射, 而图 X 和图 X' 称为是同构的, 记作 $X \cong X'$.

图 X 到自身上的同构映射叫做图 X 的 自同构.

由上述定义可以看出，两个同构的图的邻接矩阵在顶点适当编序之下是一样的. 更一般地，容易证明

命题 1.6 *设 $\mathbf{A}$ 和 $\mathbf{A}'$ 分别是 n 点图 X 和 X' 的邻接矩阵，则 $X \cong X'$ 的充要条件是存在 $n\times n$ 置换矩阵 $\mathbf{P}$ 使 $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{A}'$.*

(证明从略.)

容易看出，图之间的同构关系是等价关系，从抽象的观点来看，同构的图可以认为是一样的. 因此，图的一个同构类可以看作是一个 (抽象的) 图.

我们还有

命题 1.7 *图 X 的全体自同构的集合在映射乘法之下组成一个群，叫做图 X 的自同构群，记作 $\mathrm{Aut}(X)$.*

下面引进图的顶点的*度*的概念. 设 $X=(V,E)$ 是一个无向简单图，v 是 V 中的一个顶点，则称与 v 相邻的顶点的个数 (或与 v 相关的边的个数) 为点 v 的度，记作 $d(v)$, 或更明确地记作 $d_X(v)$. 如果 X 是有自环图，比如 $(v,v)\in E$, 则规定 $d(v)$ 为与 v 相邻的顶点个数再加上 2. 设 $v=\{v_1,\cdots,v_n\}$, 则称序列 $d(v_1),\cdots,d(v_n)$ 为图 X 的*度序列* (degree sequence). 通常度序列依大小排列，即在顶点适当编序下使度序列满足

$$\delta(X)=d(v_1)\le d(v_2)\le\cdots\le d(v_n)=\Delta(X), \tag{1.1}$$

其中 $\delta(X)$ 和 $\Delta(X)$ 分别是 X 的诸顶点的度数的最小值和最大值. 我们称 0 度顶点为*孤立点*.

下面的命题是简单但重要的.

命题 1.8 *设 (1.1) 式是无向图 X 的度序列，则*

$$\sum_{i=1}^{n} d(v_i)=2\|X\|.$$

(证明请读者补足.)

在本章中，我们感兴趣的图几乎都是下面定义的 正则图.

定义 1.9 设 X 是无向简单图，如果 $\delta(X)=\Delta(X)=k$, 我们就称 X 为 k 度正则图, 而所谓 X 是 正则图, 指的是对某个非负整数 k, X 是 k 度正则图.

以上讨论的是无向图的情形. 对于有向图，情况比较复杂. 设 $X=(V,E)$ 是一个有向图， $v\in V$. 我们称以 v 为起点的有向边的个数为 v 的 出度, 记作 $d_+(v)$; 而称以 v 为终点的有向边的个数为 v 的 入度, 记作 $d_-(v)$. 容易看出，任一有向图中满足

$$\sum_{v\in V} d_+(v)=\sum_{v\in V} d_-(v). \tag{1.2}$$

我们再令 $d(v)=d_+(v)+d_-(v)$, 叫做点 v 的度数.

对有向图，也有正则图的概念.

定义 1.10 设 X 是有向简单图，如果它的任一顶点的出度和入度都等于某一非负整数 k, 则称 X 为 k 度正则有向图.

由 (1.2) 式容易看出，对于一个有向简单图，只要每点的出度或入度都相等，它们必然等于同一个数 k. 还有，和无向图不同的是，一个 k 度正则有向图，它每点的总度数是 $2k$.

下面引进有向或无向图的子图的概念.

定义 1.11 称图 $X'=(V',E')$ 为图 $X=(V,E)$ 的 子图, 如果 $V'\subseteq V$ 且 $E'\subseteq E$. 并记作 $X'\subseteq X$.

如果满足 $V'=V$, 则称 X' 为 X 的 支撑子图 (spanning subgraph). 又如果 $V'\subseteq V$, 但 E' 包含 E 中所有联结 V' 中顶点的边，则称 X' 为 X 的由 V'诱导出的子图 (subgraph induced by V'), 记作 $X'=[V']$.

设 W 是 V 的一个真子集，我们称 $[V-W]$ 为由图 X 移去顶点集 W 得到的子图, 常记作 $X-W$. 如果 $W=\{w\}$, 则记 $X-W$

为 $X-w$, 称作由 X 移去点 w 得到的图. 类似地, 若 $E'\subseteq E$, 我们规定 $X-E'=(V(X),E(X)-E')$, 叫做由 X 移去边集 E' 得到的图, 这样的图都是 X 的支撑子图.

下面的概念是十分重要的.

定义 1.12 设 X 是有向或无向图. 我们称 X 的顶点和边相间的序列

$$W=v_0e_1v_1e_2v_2\cdots v_{l-1}e_lv_l,\ v_i\in V, e_i\in E$$

为图 X 中的一个 途 (walk), 如果满足

$$e_i=(v_{i-1},v_i)\in E,\ i=1,2,\cdots,l.$$

又如果 $v_0=v_l$, 则称 W 为一个 闭途 (closed walk).

假如途 W 中诸边 $e_1,\cdots,e_l$ 互不相同, 则称途 W 为 迹 (trail), 而若又有 $v_0=v_l$, 则称 W 为 闭迹.

假如途 W 中诸顶点 $v_0,v_1,\cdots,v_l$ 互不相同, 则称途 W 为 路 (path). 而如果 $v_0=v_l$, 但 $v_1,\cdots,v_l$ 互不相同, 则称 W 为 圈 (cycle).

由于途中诸顶点互不相同显然可推出诸边也互不相同, 因此路和圈都是迹.

无论是途, 迹, 路或圈, 其中经过的边的个数 l 叫做它的 长度. 又, 为简便计, 常用

$$W=v_0v_1\cdots v_l$$

来表示一个途 (迹、路或圈), 而把其中的边省略. 这时当然要求 $(v_{i-1},v_i)\in E$.

我们常以 P_{l+1} 和 C_l 分别记长为 l 的无向路和无向圈构成的图.

注意, 上述定义对有向图也都适用. 有向圈常称为 回路.

有了上面的概念, 我们就可以引入图的 连通性 和 连通分支 的概念. 首先考虑无向图的情形.

定义 1.13 设 $X=(V,E)$ 是一个无向图. 我们在顶点集 V 上规定一个关系 "$\sim$": 对于 $u,v\in V$, 规定 $u\sim v$, 如果 $u=v$, 或者 $u\neq v$, 但至少有一条由 u 到 v 的路. 容易验证, 关系 "$\sim$" 是 V 上的等价关系, 因此把 V 分成若干个互不相交的子集的并:

$$V=V_1\cup V_2\cup\cdots\cup V_s,\ V_i\cap V_j=\varnothing,\ \forall i,j.$$

我们称导出子图 $[V_i]$ 为 X 的 *连通分支*, $i=1,2,\cdots,s$. 如果 $s=1$, 即 X 只有一个连通分支, 则称图 X 为 *连通图*.

对于有向图, 所谓它是连通的指的是它的基础无向图是连通的. 它的连通分支也由其基础无向图的连通分支来决定. 但有向图有更强的连通性概念.

定义 1.14 设 $X=(V,E)$ 是有向图, 称 X 为 *强连通的*, 如果对任意的 $u,v\in V$, $u\neq v$, 都存在一条由 u 到 v 的 (有向) 路.

强连通有向图当然是连通的, 但反过来不对, 请读者自己举例说明之.

在我们后面的讨论中十分重要的还有 *距离* 的概念.

定义 1.15 设 $X=(V,E)$ 是无向图, 我们在 V 上规定一个二元函数 $d(u,v)$, 叫做 X 的 *距离函数*, 采取如下的规定方法: 对于 $u,v\in V$, 命

$$d(u,v)=\begin{cases}0, & \text{如果 } u=v,\\ \infty, & \text{如果不存在由 } u \text{ 到 } v \text{ 的路},\\ l, & \text{如果 } l \text{ 是由 } u \text{ 到 } v \text{ 的最短路的长度}.\end{cases}$$

显然, 如上规定的距离函数是有意义的, 并且满足:

(1) $d(u,v)\geq 0$, 并且仅当 $u=v$ 时才有 $d(u,v)=0$;

(2) $d(u,v)=d(v,u)$;

(3) $d(u,v)+d(v,w)\geq d(u,w)$.

如果再假定 X 是连通的, 则 $d(u,v)$ 在 V 上将取到一个最大值 $d\neq\infty$, 我们称 $d=d(X)$ 为图 X 的 *直径*. 连通图的直径这个概念在我们今后的讨论中是十分重要的.

我们还需要下面的概念.

定义 1.16 设 $X=(V,E)$ 是无向简单图, 如果 X 中没有圈, 则称 X 为 **林** (forest) 或 **无圈图** (acyclic graph). 又若 X 是连通的, 则称 X 为 **树** (tree).

下面的定理给出树的几个等价的定义.

定理 1.17 设 X 是无向简单图, 则下述事项等价:

(1) X 是树;

(2) X 的任意二点间有唯一的一条路;

(3) X 连通且 $|X|=\|X\|+1$;

(4) X 无圈且 $|X|=\|X\|+1$.

(证明从略)

定义 1.18 设 X 是无向简单图, 并且 X 中有圈. 我们以 $g(X)$ 记 X 中最短圈的长度, 叫做 X 的 **围长** (girth); 而以 $c(X)$ 记 X 中最长圈的长度, 叫做 X 的 **周长** (circumference).

显然有

$$3\le g(X)\le c(X)\le |X|.$$

定义 1.19 设 $X=(V,E)$ 是无向图, 我们以 E 作为顶点集如下规定一个图 $L(X)$: 对于 $e_1,e_2\in E$, 则 (e_1,e_2) 是 $L(X)$ 的边 $\Longleftrightarrow$ e_1,e_2 在 X 中有公共的端点, 这样的图 $L(X)$ 叫做 X 的 **线图** (line graph).

线图的概念在构造一些具有高度对称性的图的例子时很有用处.

定义 1.20 设 $X=(V,E)$ 是无向简单图, 称图 $\overline{X}=(V,V^{\{2\}}-E)$ 为 X 的 **补图** (complement).

而对有向简单图 $X=(V,E)$, 定义 X 的补图为 $\overline{X}=(V,V^{(2)}-E)$.

在本节的最后，我们介绍图的几种运算. 首先介绍两个图的**并**和**联**.

设 $X=(V,E)$ 和 $X'=(V',E')$ 是任意两个有向或无向图. 则规定 $X\cup X'=(V\cup V',E\cup E')$, 叫做 X 和 X' 的**并** (union). 如果在 $X\cup X'$ 上再添加连结 V 的任一个顶点和 V' 的任一个顶点的所有的边，这样得到的图记作 $X+X'$, 叫做 X 和 X' 的**联** (join). 设 k 是一个正整数，我们以 kX 表 k 个顶点集互不相交的同构于 X 的图的并，有时也记作 $X\cup X\cup\cdots\cup X$. 因为我们总约定，在作并和联的运算时，只要二图不是某个预先指定的更大的图的子图，则认为它们的顶点集是互不相交的.

并和联这两种运算与补有下面的关系：只要 X 和 X' 顶点集互不相交，则有

$$\overline{X\cup X'}=\overline{X}+\overline{X}',\qquad \overline{X+X'}=\overline{X}\cup\overline{X}'.$$

下面介绍几种以后常用的图.

设 V 是 n 点有限集，则称图 $(V,V^{\{2\}})$ 为 n 点**完全图**, 记作 K_n, 它有 $\binom{n}{2}$ 条边.

K_n 的补 $\overline{K}_n$ 系由 n 个孤立点组成，叫做 n 点**空图**, 记作 E_n 或 nK_1, 它的边集是空集.

$K_1=E_1$ 叫做**平凡图**.

对任意的正整数 m,n, 命 $K_{m,n}=E_m+E_n$, 叫做 (m,n) 型**完全二部图**. (称简单无向图 $X=(V,E)$ 为**二部图**, 如果 $V=V_1\cup V_2$, 且 $V_1\cap V_2=\varnothing$, 但 $V_1\neq\varnothing$, $V_2\neq\varnothing$, 满足下述条件：对任一 $e=(v_1,v_2)\in E$, 必有 $v_1\in V_1$, $v_2\in V_2$.)

又若 $n_1,\cdots,n_r$ 为正整数，命 $K_{n_1,\cdots,n_r}=E_{n_1}+\cdots+E_{n_r}$, 叫做 $(n_1,\cdots,n_r)$ 型**完全 r-部图**.

最后我们介绍两个图的**笛卡儿积**和**字典式积**.

设 $X=(V,E)$ 和 $X'=(V',E')$ 是任意两个有向或无向图. 则规定 X 和 X' 的笛卡儿积 $X\times X'$ 为具有顶点集合 $V\times V'$ 的图，满足 (x,x') 和 (y,y') 相邻当且仅当 $x=y$ 且 $(x',y')\in E(X')$, 或者 $x'=y'$ 且 $(x,y)\in E(X)$. 再规定 X 和 X' 的字典式积 $X[X']$

为具有顶点集合 $V \times V'$ 的图，满足 (x, x') 和 (y, y') 相邻当且仅当 $(x, y) \in E(X)$，或者 $x = y$ 且 $(x', y') \in E(X')$.

根据这个定义，完全二部图 $K_{n,n} = K_2[nK_1]$，而 $C_4 = K_2 \times K_2$.

关于图论一般知识的参考书有

1. B. Bollobás, *Graph Theory*, Springer-Verlag, 1979.

2. J.A. Bondy and U.S.R. Murty, *Graph Theory with Applications*, American Elsevier Publishing Co., Inc., 1976.

3. F. Harary, *Graph Theory*, Addison-Wesley, 1969.

习　题

1. 证明定理 1.17.

2. 称 n 阶有向图 X 为 *竞赛图*，如果对任意的两点 $u, v \in V(X)$，(u, v) 与 (v, u) 二弧中有且仅有一条弧属于 $E(X)$. 证明竞赛图的自同构群必为奇数阶.

§2. 图的谱和邻接代数

在系统讲述群与图的理论之前，我们简单介绍一下图的谱和邻接代数的概念. 它们的深入讨论将用到群表示论.

在本节中，我们考虑的矩阵和多项式都是在复数域 $\mathbb{C}$ 上的. 以 $\mathbf{I}$(或更明确地，$\mathbf{I}_n$) 表 n 阶单位矩阵，以 $\mathbf{J}$ 表 n 阶全 1 矩阵. 以 $\mathbf{A}^t$ 表 $\mathbf{A}$ 的转置. 以 $f_{\mathbf{A}}(\lambda) = |\lambda \mathbf{I} - \mathbf{A}|$ 表矩阵 A 的特征多项式 (并经常简记作 $f(\lambda)$).

设 $X = (V, E)$ 是一个 (有向或无向，简单或有自环) 图，$\mathbf{A}$ 是它的邻接矩阵. 我们称 $f_{\mathbf{A}}(\lambda)$ 为图 X 的 *特征多项式*，(因此有时也记作 $f_X(\lambda)$)，并称 $f(\lambda)$ 的全部特征根 $(\lambda_1, \cdots, \lambda_n)$ 为图 X 的 *谱*.

前面提到，图的邻接矩阵并不唯一确定. 如果改换图的诸顶点的编号，邻接矩阵 $\mathbf{A}$ 将会变成 $\mathbf{P}^{-1}\mathbf{AP}$，其中 P 是适当的置换矩阵. 但是，它们的特征多项式则是一样的. 因此，$f_X(\lambda)$ 和图的谱 $\mathrm{spec}(X) = (\lambda_1, \cdots, \lambda_n)$ 都是被图 X 唯一确定的.

为了便于较深入的讨论，并从中突出谱分析对图论的意义，我们在以下只局限于讨论无向简单图.

由现在起，我们总假定 $X=(V,E)$ 是一个无向简单图，并且 $|X|=n$, $\|X\|=m$. X 的邻接矩阵 $\mathbf{A}$ 一定是一个主对角线元素皆为 0 的对称 $(0,1)$ 矩阵.

由初等线性代数我们知道，如果把 $\mathbf{A}$ 看成是复数域上的矩阵，它的诸特征值都是实数，并且可用实正交变换把它变成对角形，其对角元素就是这些特征值. 假定这些特征值依大小次序排列是

$$\lambda_0>\lambda_1>\cdots>\lambda_{s-1},\ s\le n,$$

并且 λ_i 的重数是 $m(\lambda_i)=m_i$, 则我们常把图 X 的谱记作

$$\operatorname{spec}(X)=\begin{pmatrix}\lambda_0 & \lambda_1 & \cdots & \lambda_{s-1}\\ m_0 & m_1 & \cdots & m_{s-1}\end{pmatrix}, \tag{2.1}$$

而把 X 的特征多项式记作

$$f_X(\lambda)=\lambda^n+c_1\lambda^{n-1}+c_2\lambda^{n-2}+\cdots+c_n. \tag{2.2}$$

明显地，$f(\lambda)$ 是整系数的首 1 多项式，因此它的特征根全是代数整数.

有时我们还考虑 $\mathbf{A}$ 的极小多项式 $g_{\mathbf{A}}(\lambda)$, 它也是由图 X 唯一确定的，因此也记作 $g_X(\lambda)$, 并常简记作 $g(\lambda)$. 因为 $\mathbf{A}$ 是实对称矩阵，$g(\lambda)$ 也是整系数首 1 多项式，并且

$$g(\lambda)=(\lambda-\lambda_0)(\lambda-\lambda_1)\cdots(\lambda-\lambda_{s-1}). \tag{2.3}$$

图的特征多项式 (2.2) 的系数有明显的几何意义，比如我们有

命题 2.1 设 (2.2) 式是无向简单图 X 的特征多项式，则

(1) $c_1=0$;

(2) $-c_2=\|X\|$;

(3) $-c_3$ 是 X 中 C_3 型子图个数的 2 倍.

证 由初等线性代数，对于 $i=1,2,\cdots,n$, c_i 等于 $\mathbf{A}$ 的所有 i 阶主子式的和再乘上 $(-1)^i$. 于是有

(1) $c_1=-\mathrm{tr}\ \mathbf{A}=0$.

(2) c_2 是 $\mathbf{A}$ 的所有 2 阶主子式的和. 2 阶主子式有两种类型，即

$$\begin{vmatrix}0&0\\0&0\end{vmatrix} \quad \text{和} \quad \begin{vmatrix}0&1\\1&0\end{vmatrix},$$

后者对应着图 X 中的一条边，但因

$$\begin{vmatrix}0&1\\1&0\end{vmatrix}=-1,$$

于是

$$c_2=-\|X\| \quad \text{或} \quad -c_2=\|X\|.$$

(3) $\mathbf{A}$ 的三阶主子式共有以下八种类型：

$$\begin{vmatrix}0&0&0\\0&0&0\\0&0&0\end{vmatrix},\begin{vmatrix}0&0&1\\0&0&0\\1&0&0\end{vmatrix},\begin{vmatrix}0&1&0\\1&0&0\\0&0&0\end{vmatrix},\begin{vmatrix}0&0&0\\0&0&1\\0&1&0\end{vmatrix},$$

$$\begin{vmatrix}0&1&1\\1&0&0\\1&0&0\end{vmatrix},\begin{vmatrix}0&0&1\\0&0&1\\1&1&0\end{vmatrix},\begin{vmatrix}0&1&0\\1&0&1\\0&1&0\end{vmatrix},\begin{vmatrix}0&1&1\\1&0&1\\1&1&0\end{vmatrix}.$$

除最后一个的值

$$\begin{vmatrix}0&1&1\\1&0&1\\1&1&0\end{vmatrix}=2$$

外，其余都等于 0. 这最后一种类型对应着图 X 中的一个三角，即 C_3 型子图，故 $c_3=(-1)^3\cdot 2\cdot X$ 中的三角数. 即 $-c_3=2\cdot X$中三角数. □

根据邻接矩阵 $\mathbf{A}=(a_{ij})$ 的定义，元素 a_{ij} 等于连接 v_i 和 v_j 两顶点的边数，(这个数为 0 或 1)，推广到 $\mathbf{A}$ 的方幂，我们有

命题 2.2 设 l 是正整数，则 $\mathbf{A}^l$ 的 (i,j)-元素等于由 v_i 到 v_j 的长度为 l 的途的个数.

证 用对 l 的归纳法. 当 $l=1$ 时，由 $\mathbf{A}$ 的定义即得结论. 当 $l>1$ 时，因为

$$(\mathbf{A}^{l+1})_{ij}=\sum_{k=1}^{n}(\mathbf{A}^l)_{ik}a_{kj},$$

由归纳假设，即得结论. □

在图的代数化研究中，下面的概念也起着重要的作用.

定义 2.3 设 $\mathbf{A}$ 是图 X 的邻接矩阵. 令

$$\mathcal{A}(X)=\{f(\mathbf{A})\mid f(\lambda)\in\mathbb{C}[\lambda]\}.$$

则 $\mathcal{A}(X)$ 是全矩阵代数 $M_n(\mathbb{C})$ 的子代数，叫做图 X 的 (关于邻接矩阵 $\mathbf{A}$ 的) 邻接代数 (adjacency algebra).

注意，邻接代数是依赖于邻接矩阵 $\mathbf{A}$ 的.

明显的，若 $\mathbf{A}$ 的极小多项式 $g(\lambda)$ 次数为 s, 则 $\mathbf{I},\mathbf{A},\cdots,\mathbf{A}^{s-1}$ 线性无关，于是 $\mathcal{A}(X)$ 的维数 $\dim\mathcal{A}(X)=s$, 这个数并不依赖于 $\mathbf{A}$ 的特殊选择. 显然， $\dim\mathcal{A}(X)\le n$.

对于连通图来说， $\dim\mathcal{A}(X)$ 与 X 的直径 d 有下述关系:

命题 2.4 设 X 是连通图, d 是 X 的直径. 则 $\dim\mathcal{A}(X)\ge d+1$.

证 只须证明 $\mathbf{I},\mathbf{A},\cdots,\mathbf{A}^d$ 在 $\mathcal{A}(X)$ 中是线性无关的.

因为 X 是连通的且直径为 d, 必有 $d\le n-1$, 并且存在两点 x,y 使 $d(x,y)=d$, 并存在由 x 到 y 的长为 d 的路 W. 设 $W=v_1v_2\cdots v_{d+1}$ 是一条这样的路，其中 $v_1=x,v_{d+1}=y$. 于是，对 $i=2,3,\cdots,d+1$, 存在由 v_1 到 v_i 的长为 $i-1$ 的路，但不存在长度更短的路. 这说明

$$(\mathbf{A}^{i-1})_{1i}\neq 0,\quad 但\ (\mathbf{A}^j)_{1i}=0,\ 对 j<i-1.$$

于是 $\mathbf{A}^{i-1}$ 和 $\{\mathbf{I}, \mathbf{A}, \cdots, \mathbf{A}^{i-2}\}$ 线性无关. 这样, 用对 i 的归纳法, 即可证明 $\{\mathbf{I}, \mathbf{A}, \cdots, \mathbf{A}^{d}\}$ 的线性无关性. □

注意到邻接代数的维数 s 为 X 的不同的特征值的个数, 则有

推论 2.5 *设 X 是 n 点连通图, 直径为 d. 则 X 的不同的特征值的个数在 $d+1$ 和 n 之间.*

一个有趣的问题是研究恰有 $d+1$ 个不同特征值以及恰有 n 个不同特征值的图的性质. 完全决定这些图则是一个相当困难的问题.

对于正则图的谱和邻接代数有下面的

命题 2.6 *设 $X=(V,E)$ 是 k 度正则图, 则*

(1) k 是 X 的一个特征值;

(2) 若 X 连通, 则 k 的重数为 1;

(3) 对 X 的任一特征值 λ, 有 $|\lambda| \le k$.

证 (1) 令 $\mathbf{A}$ 是 X 的邻接矩阵, 又令 n 维向量

$$\alpha = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

则 $\mathbf{A}\alpha = k\alpha$, 故 k 是 $\mathbf{A}$ 的特征值.

(2) 设 $\alpha=(a_1, a_2, \cdots, a_n)^t$ 是 $\mathbf{A}=(a_{ij})$ 的属于 k 的特征向量, 并设 a_i 是绝对值最大的坐标, 当然 $a_i \ne 0$. 则由 $\mathbf{A}\alpha = k\alpha$ 推知 (比较第 i 个坐标)

$$\sum_{j=1}^{n} a_{ij}a_j = ka_i.$$

因为在 $\mathbf{A}$ 的第 i 行中恰有 k 个元素不为 0, 上式就推出对应这些元素的 a_j 都等于 a_i. 更明确地, 我们推出, 若 v_j, v_i 相邻, 则 $a_j = a_i$. 由此即得: 若 X 连通, 则 α 的每个坐标皆为 a_i, 于是

$\alpha = a_i(1, 1, \cdots, 1)^t$. 这样，对应于特征值 k 的特征子空间是 1 维的. 由 $\mathbf{A}$ 对称，即得 k 的重数为 1.

(3) 设 $\beta = (b_1, \cdots, b_n)^t \neq 0$ 是 $\mathbf{A}$ 的属于特征值 λ 的特征向量，于是 $\mathbf{A}\beta = \lambda\beta$. 再设 b_i 是 β 的绝对值最大的坐标，于是有

$$\sum_{j=1}^{n} a_{ij} b_j = \lambda b_i.$$

取绝对值得

$$|\lambda||b_i| \le \sum_{j,\ 使\ a_{ij}=1} |b_j| \le k|b_i|,$$

其中 $\sum$ 在所有使 $a_{ij} = 1$ 的 j 上求和. 由 $|b_i| \neq 0$, 就推出 $|\lambda| \le k$. □

正则连通图的邻接代数有下列重要性质.

定理 2.7 (Hoffman) X 是正则连通图 $\iff$ $\mathbf{J} \in \mathcal{A}(X)$, 其中 $\mathbf{J}$ 是全 1 矩阵.

证 $\Longleftarrow$: 若 $\mathbf{J} \in \mathcal{A}(X)$, 则 $\mathbf{J}$ 是邻接矩阵 $\mathbf{A}$ 的多项式，于是 $\mathbf{JA} = \mathbf{AJ}$. 因为左边的 (i,j)-元素是 v_j 的度数 k_j, 而右边的 (i,j) 元素是 v_i 的度数 k_i, 于是有 $k_i = k_j$, $\forall i, j$. 即 X 是正则图.

又若 X 非连通，则存在两点 v_i, v_j, $i \neq j$, 之间没有路相连，当然也没有途相连. 因此，由命题 2.2, 对任意的正整数 l, $\mathbf{A}^l$ 的 (i,j)-元素皆为 0, 于是 $\mathbf{A}$ 的任一多项式 $f(\mathbf{A})$ 的 (i,j)-元素也为 0, 与 $\mathbf{J} \in \mathcal{A}(X)$ 矛盾.

$\Longrightarrow$: 设 X 是 k 度正则连通图. 由命题 2.6, k 是 X 的特征根. 可设 $\mathbf{A}$ 的极小多项式为

$$g(\lambda) = (\lambda - k)q(\lambda),$$

于是有 $\mathbf{A}q(\mathbf{A}) = kq(\mathbf{A})$, 这说明 $q(\mathbf{A})$ 的诸列向量皆为 $\mathbf{A}$ 的对应于 k 的特征向量或零向量. 但因 k 的重数为 1, 诸列皆为 $(1, 1, \cdots, 1)^t$ 的倍数. 又由 $q(\mathbf{A}) \neq 0$, 及 $q(\mathbf{A})$ 的对称性有 $q(\mathbf{A})$ 是 $\mathbf{J}$ 的非 0 倍数. 于是 $\mathbf{J} \in \mathcal{A}(X)$. □

对于 k 度正则连通图，我们进一步有

推论 2.8 设 X 是 n 阶 k 度正则连通图，其不同的特征值为 $k > \lambda_1 > \cdots > \lambda_{s-1}$. 命

$$q(\lambda) = \prod_{i=1}^{s-1}(\lambda - \lambda_i),$$

则 $\mathbf{J} = (\frac{n}{q(k)})q(\mathbf{A})$.

证 在定理 2.7 的证明中我们已得出 $q(\mathbf{A}) = c\mathbf{J}$, $c \neq 0$. 因为 $\mathbf{A}$ 的不同特征值为 $k, \lambda_1, \cdots, \lambda_{s-1}$, 故 $q(\mathbf{A})$ 的特征值为 $q(k)$ 和 $q(\lambda_i)$. 由 $q(\lambda)$ 的表达式，$q(\lambda_i) = 0, i = 1, \cdots, s-1$. 又因 $c\mathbf{J} = q(\mathbf{A})$ 的仅有的非零特征值为 cn, 于是必有 $cn = q(k)$, 推出 $c = \frac{q(k)}{n}$. 由此即得 $\mathbf{J} = (\frac{n}{q(k)})q(\mathbf{A})$. □

注 2.9 (1) 由矩阵论中的 Frobenius 定理，任一非负矩阵 $\mathbf{A}$ 都有一个非负特征值 λ_0, 使得 $\mathbf{A}$ 的任一特征值都在以原点为心，λ_0 为半径的园内. 对于图的邻接矩阵来说，这个 λ_0 叫做图 (或其邻接矩阵) 的 指标 (index).

(2) 命题 2.6 告诉我们，对于 k 度正则图来说，其指标 $\lambda_0 = k$. 对于一般的简单无向图，如何给出指标 λ_0 的一个上界，这是个有趣的问题. 本节后面的习题将给出一个估值.

计算一个给定图的谱一般来说是十分困难的. 在 Biggs 书第三章有所谓循环图的谱的计算，以及几种特殊类型的图的谱，请读者参考该书.

又，由图的谱来刻划图也是谱分析的一个重要方向，见 Biggs 书 §3D.

关于图的谱分析有一个著名的未解决问题，即所谓决定 整谱 图 的问题，这是 F. Harary 和 A.J. Schwenk 在 “Which graphs have integral spectra?” (见 “Graphs and Combinatorics”, Lecture Notes in Math. No. 406, 1974, pp. 45–51) 中提出的. D.M. Cvetković 在 “Cubic integral graphs” 一文 (Univ. Beograd Publ. Elektrotehn.

Fak., Ser. Mat. Fiz., No. 498–541 (1975), pp. 107–113) 中证明，给定度数的正则连通整谱图只有有限多个，并且定出了所有 3 度正则连通整谱图 (共有 13 个). 亦可见 Schwenk 的 "Exactly 13 connected cubic graphs have integral spectra" (见 "Theory and Applications of Graphs", (Proc. Kalamazoo, 1976), Springer-Verlag, 1978, 516–533.

谱分析的主要参考书是下面的

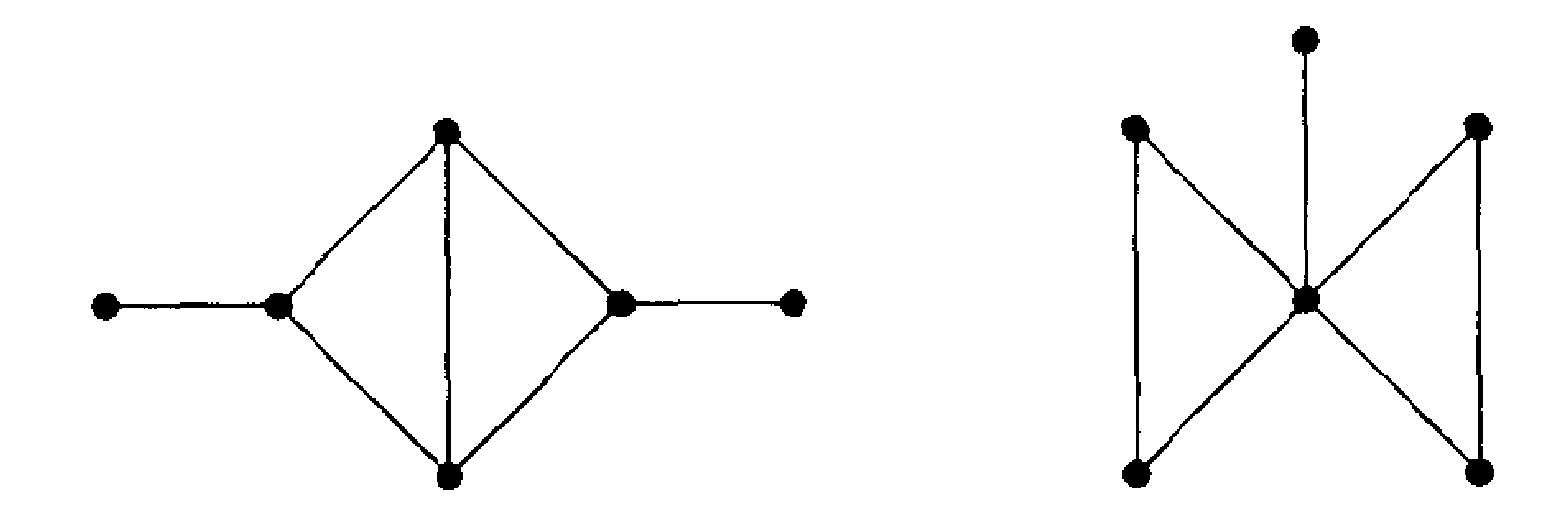
D.M. Cvetković, M. Doob, H. Sachs, *Spectra of Graphs — Theory and Application*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1980.

在该书最后提出几个未解决问题，其中之一是决定所有特征值互不相同的图. 这是个值得研究的问题.

习 题

1. 设 $\mathbf{A}$ 是 n 点无向简单图 X 的邻接矩阵. 则 X 连通 $\Longleftrightarrow$ $(\mathbf{A}+\mathbf{I})^{n-1}$ 的任一元素皆不为 0.

2. 验证下面二图的特征多项式相同，并计算它的特征多项式及谱.



这样的两个图叫做 **同谱图** (cospectral graphs).

3. 设 X 是简单无向图， $|X|=n$, $\|X\|=m$, 其特征值依大小排列是 $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. 则

(1) $\sum_{i=1}^{n} \lambda_i = 0$, $\sum_{i=1}^{n} \lambda_i^2 = 2m$.

(2) 证明 $\lambda_1 \leq (\frac{2m(n-1)}{n})^{\frac{1}{2}}$.

§3. 图的自同构群

在 §1 中我们定义了两个图同构，图的自同构以及自同构群的概念，见定义 1.5 和命题 1.7. 本节我们将继续研究图的自同构

和自同构群. 首先再明确地给出图的自同构和自同构群的定义.

定义 3.1 设 $X=(V,E)$ 是一个 (有向或无向) 图, α 是集合 V 的置换. 称 α 为图 X 的 *自同构*, 如果 $(u,v)\in E \iff (u^\alpha,v^\alpha)\in E$.

图 X 的所有自同构在置换乘法之下组成一个群, 叫做 X 的 *自同构群*, 记作 $\mathrm{Aut}(X)$. 它是集合 V 上的置换群.

两个同构的图有同构的自同构群, 更明确地, 我们有

命题 3.2 设 $\sigma: V\to V'$ 是 $X=(V,E)$ 到 $X'=(V',E')$ 上的同构, 则

$$\mathrm{Aut}(X')=\sigma^{-1}\mathrm{Aut}(X)\sigma.$$

(验证从略.)

由于图的自同构保持顶点间的相邻关系, 因此它也可看成是 $E(X)$ 上的置换. 由 $\mathrm{Aut}(X)$ 诱导出的 $E(X)$ 上的置换群记作 $\mathrm{Aut}_E(X)$. 但应注意, 一般不一定有 $\mathrm{Aut}(X)\cong\mathrm{Aut}_E(X)$. 最简单的例子是完全图 K_2, $\mathrm{Aut}(K_2)=S_2$, 但 $\mathrm{Aut}_E(K_2)=1$. Sabidussi 证明了, 对无向简单图 X 来说, $\mathrm{Aut}(X)\cong\mathrm{Aut}_E(X)\iff X$ 至多有一个孤立点, 且 K_2 不是 X 的连通分支. 证明可见 Harary 的《图论》定理 14.1.

下面看一些例子, 证明都留给读者.

例 3.3 (1) $\mathrm{Aut}(K_n)=\mathrm{Aut}(\overline{K}_n)=S_n$.

(2) 对任一 (无向或有向) 简单图 X, 有 $\mathrm{Aut}(X)=\mathrm{Aut}(\overline{X})$.

(3) 若 $\mathrm{Aut}(X)=1$, 则称 X 为幺图. 证明下面的图 X_1 和 X_2 都是幺图, 并且 X_2 是点数最少的非平凡无向简单幺图.

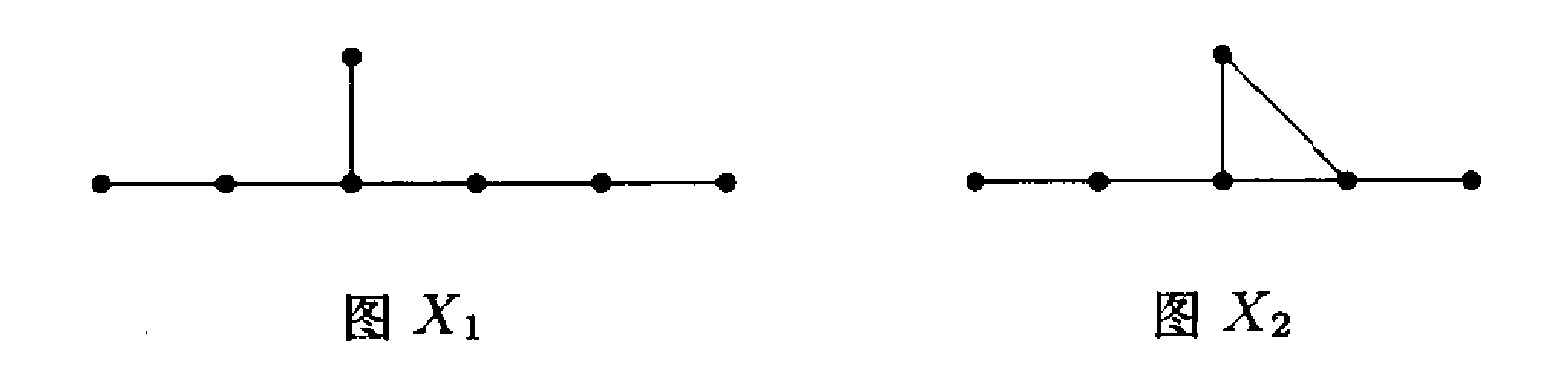


图 X_1　　图 X_2

(4) $\mathrm{Aut}(K_4)$ 在边集 $E(K_4)$ 上诱导的置换群 $\mathrm{Aut}_E(K_4) \le S_6$, 它是 K_4 的线图 $L(K_4)$ 的自同构群 $\mathrm{Aut}(L(K_4))$ 的子群. 问 $\mathrm{Aut}_E(K_4)$ 和 $\mathrm{Aut}(L(K_4))$ 是否相等?

(5) 设 X 是一连通图. 以 nX 表 n 个 X 的并. 则

$$\mathrm{Aut}(nX) = \mathrm{Aut}(X) \wr S_n,$$

其中 "$\wr$" 表群的圈积. (参见 III,§5). 注意, 如果 X 不是连通图, 则结论不真, 试举例说明之.

以下我们开始讨论图的对称性, 首先有下面的

定义 3.4 图 X 的两个顶点 u, v 叫做*相似的* (similar), 如果存在 $\alpha \in \mathrm{Aut}(X)$ 使 $u^\alpha = v$.

形象地说, 从图 X 的两个相似顶点 u, v 的角度去看这个图, 结果是一样的. 或者说, u, v 两点在图 X 中的地位是对称的.

以下我们感兴趣的图主要是具有高度对称性的图. 通常图的对称性的描述是通过它的自同构群, 特别是自同构群的某种传递性质. 下面我们给出对研究图的对称性极为重要的若干基本概念.

定义 3.5 称无向或有向图 X 为*点传递图*, 如果 $\mathrm{Aut}(X)$ 在 $V(X)$ 上是传递置换群.

定义 3.6 称无向或有向图 X 为*边传递图*, 如果 $\mathrm{Aut}_E(X)$ 在 $E(X)$ 上是传递置换群.

对于无向图 X, 我们把每个无向边 $\{u, v\}$ 看作两个有向边 (u, v) 和 (v, u), 这些有向边叫做无向图 X 的*弧*. (对于有向图来说, 我们有时也把它的边叫做弧.) 考虑 X 的自同构群 $\mathrm{Aut}(X)$ 在 X 的全体弧的集合上的作用, 我们有下面的

定义 3.7 称无向或有向图 X 为*弧传递图*，如果 X 无孤立点，并且 $\mathrm{Aut}(X)$ 在 X 的弧集上的作用是传递的. 弧传递图也叫对称图.

以上定义的这三种传递性是最基本的传递性，其中以弧传递性为最强. 显然它可推出点传递性和边传递性. 但点传递性和边传递性二者不能互相推出. 而且一个点传递且边传递的无向图也不一定是弧传递的，这点以后我们还要提到. 这里，请读者先试着举些例子来说明这些传递性之间的关系. 点传递但不边传递的例子容易举出，对于边传递但不点传递的无向图我们有下面的

定理 3.8 *设 X 是无孤立点的边传递但不点传递的简单无向图，则 X 必为二部图.*

证 任取 $(u,w)\in E(X)$，并设 U 和 W 是 $V=V(X)$ 的包含 u 和 w 的轨道. 由 X 无孤立点和边传递性得 $U\cup W=V$. 再由 $\mathrm{Aut}(X)$ 不点传递，必有 $U\cap W=\varnothing$. 最后，再用边传递性，推得 X 的每条边均连结 U 中的一顶点和 W 中的一顶点，即 X 是二部图. □

事实上，对于 $m\neq n$, $K_{m,n}$ 就是边传递但不点传递的无向图的典型例子.

另外， Bouwer 举出了一个边传递但不点传递的正则图的例子，见他的 "On edge but not vertex transitive regular graphs, *J. Combin. Th. Ser. B*, **12** (1972), 32–40". 这种图今天叫做*半对称图*，我们在 §6 中还要提到.

应该指出，图的传递性和连通性之间一般来说是没有关系的. 由图 X 的点传递性或边传递性都不能得到 X 的连通性. 一个平凡的例子是 E_n，它的自同构群是 S_n. 我们还可以用下述简单事实来说明：由例 3.3(5)，任取 X 为点传递 (或边传递) 的连通图，则 nX 仍为点传递 (或边传递) 的. 这就说明了点传递图和边传递图都不一定是连通的.

在引进图的一些更强的传递性之前，我们从矩阵的观点再来讨论一下图的自同构.

定理 3.9 设 $X=(V,E)$ 是图, $V=\{v_1,\cdots,v_n\}$, π 是 V 的置换. 令 $\mathbf{A}$ 是 X 的邻接矩阵. 又令 $\mathbf{P}=(p_{ij})$ 是 π 所对应的置换矩阵, 其中

$$p_{ij}=\begin{cases}1, & 若\ v_i^\pi=v_j,\\ 0, & 其它情形.\end{cases}$$

则 $\pi\in\mathrm{Aut}(X)\iff\mathbf{PA}=\mathbf{AP}$ (或 $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{A}$).

证 设 $v_i^\pi=v_h$, $v_j^\pi=v_k$, 则有

$$(\mathbf{AP})_{ik}=\sum_s\mathbf{A}_{is}\mathbf{P}_{sk}=a_{ij},$$

$$(\mathbf{PA})_{ik}=\sum_t\mathbf{P}_{it}\mathbf{A}_{tk}=a_{hk}.$$

于是 $\mathbf{AP}=\mathbf{PA}\iff a_{ij}=a_{hk},\ \forall i,j\iff(v_i,v_j)$ 与 (v_h,v_k) 同时为 X 的边或同时不为 X 的边 $\iff\pi\in\mathrm{Aut}(X)$. □

上述定理对于有重边的图 (有向或无向) 亦成立.

下面转而研究图的谱和自同构的关系.

引理 3.10 设 $X=(V,E)$ 是无向图, $\mathbf{A}$ 是它的邻接矩阵. 又设 λ 是 $\mathbf{A}$ 的重数为 1 的特征根, α 是对应于 λ 的特征向量, 而 $\mathbf{P}$ 是 X 的自同构 π 的置换矩阵, 则 $\mathbf{P}\alpha=\pm\alpha$.

证 因为 X 是无向图, $\mathbf{A}$ 是实对称矩阵, 于是 $\mathbf{A}$ 的特征值皆为实数, 并可取特征向量 α 为实向量 (坐标皆为实数). 因为 $\mathbf{P}$ 代表 X 的自同构, 由定理 3.9, 有 $\mathbf{AP}=\mathbf{PA}$, 于是 $\mathbf{P}\alpha$ 也是 $\mathbf{A}$ 的对应于 λ 的特征向量. 再由 λ 的重数为 1, 有 $\mathbf{P}\alpha=\mu\alpha$, 且 μ 为实数. 又因 $\mathbf{P}$ 是置换矩阵, 存在 $s\in\mathbb{Z}$ 使 $\mathbf{P}^s=\mathbf{I}$, 于是 $|\mu|=1$, 即 $\mu=\pm1$. □

定理 3.11 设 $X=(V,E)$ 是无向图. 设 X 的特征值重数皆为 1, 则 $\mathrm{Aut}(X)$ 为初等交换 2-群.

证 设 $\lambda_1\cdots,\lambda_n$ 是 X 的全部特征根，对应的特征向量为 $\alpha_1,\cdots,\alpha_n$. 由诸特征根重数皆为 1, 有 $\alpha_1,\cdots,\alpha_n$ 是 $\mathbb{R}^n$ 的一组基. 设 $\pi\in\mathrm{Aut}(X)$, $\mathbf{P}$ 是对应的置换矩阵. 则由引理 3.10, $\mathbf{P}\alpha_i=\pm\alpha_i$, 于是 $\mathbf{P}^2\alpha_i=\alpha_i$, $\forall i$. 由此得 $\mathbf{P}^2=\mathbf{I}$, 即 $\pi^2=1$. 这说明 $\exp\mathrm{Aut}(X)=2$, 于是 $\mathrm{Aut}(X)$ 是初等交换 2-群. □

推论 3.12 设 X 是无向图，$\mathrm{Aut}(X)$ 有一个阶 >2 的元素，则 X 有重数 >1 的特征值.

以上结果还可推广为

定理 3.13 设 X 是图 (有向或无向，有自环或有重边), $\mathbf{A}$ 是其邻接矩阵. 若 $\mathbf{A}$ 的特征根重数均为 1, 则 $\mathrm{Aut}(X)$ 是交换群.

证 因为 $\mathbf{A}$ 有 n 个不同的特征值，故在复数域上，存在 n 阶矩阵 $\mathbf{T}$ 使得

$$\mathbf{T}^{-1}\mathbf{A}\mathbf{T}=\begin{pmatrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{pmatrix}=\mathbf{D}.$$

因为诸 λ_i 互不相同，与 $\mathbf{D}$ 可交换的矩阵皆为对角形. 现在设 $\mathbf{B}_1,\mathbf{B}_2$ 与 $\mathbf{A}$ 可换，于是 $\mathbf{T}^{-1}\mathbf{B}_1\mathbf{T}$ 和 $\mathbf{T}^{-1}\mathbf{B}_2\mathbf{T}$ 与 $\mathbf{D}$ 可换，这样 $\mathbf{T}^{-1}\mathbf{B}_1\mathbf{T}$ 和 $\mathbf{T}^{-1}\mathbf{B}_2\mathbf{T}$ 就为对角形，并因此它们之间也可交换. 这又推出 $\mathbf{B}_1,\mathbf{B}_2$ 可换. 若取 $\mathbf{B}_1,\mathbf{B}_2$ 为 $\mathrm{Aut}(X)$ 中的二自同构对应的置换矩阵，就得到 $\mathrm{Aut}(X)$ 的交换性. □

用上述方法也可以给定理 3.11 一个简单证明，这作为习题留给读者.

还可定义图 X 的*中心化代数* $C(X)$ 为与 $\mathbf{A}$ 可交换的矩阵全体，它是复数域 (或实数域) 上 n 阶全矩阵代数的子代数，再定义 $C(X)$ 中全体可逆矩阵组成的乘法群为 X 的*中心化群*. 对图的中心化代数和中心化群的研究也能够并已经得出关于图的很多新结果. 这里不再赘述.

下面再看一下图的自同构群的更强的传递性. 首先我们有

定理 3.14 设 n 阶图 X 的自同构群 $\mathrm{Aut}(X)$ 在 $V(X)$ 上作用双重传递, 则 $X=K_n$ 或 nK_1.

(证明从略.)

再考虑自同构群在边集上的双传递作用. 由于边传递图加上若干孤立点之后仍为边传递图, 我们在下述定理中作了无孤立点的假设.

定理 3.15 设图 X 无孤立点, 且它的自同构群 $\mathrm{Aut}_E(X)$ 在 $E(X)$ 上作用双重传递, 则 $X=nK_2$, 或 $K_{1,n}$, 或 K_3.

证 首先设图 X 有两个或以上的连通分支, 则每个连通分支只能是 K_2. 若否, 我们在一个分支中取二相关联的边, 又在两个不同分支中各取一条边, 它们当然不相关联. 于是不存在图的自同构把第一对边变成第二对边, 与 $\mathrm{Aut}_E(X)$ 在 $E(X)$ 上双传递相矛盾. 这时有 $X=nK_2$, 第一种情形发生. 现在可设图 X 是连通图, 且 $E(X)$ 中至少含有两条边. 还用前面的推理, 因二关联的边不能变成二不关联的边以及 $\mathrm{Aut}_E(X)$ 的双传递性推知 X 中任二边皆关联. 如果 X 中有圈, 则任一圈的长只能为 3. 再进一步推出 $X=K_3$, 即在一个长为 3 的圈之外不能再有其它的边, 第二种情形发生. 最后设 X 是树. 因树中有一度顶点, 边传递性就推出 $E(X)$ 中每条边都有一个端点是一度顶点, 由此不难推出 $X=K_{1,n}$, 第三种情形发生. □

由上述两个定理看出, 图的自同构群如果在点集或边集上双传递, 则这些图都很容易决定. 于是我们可在以下假定图的自同构群是单传递置换群.

我们在第 XII 章研究过本原置换群, 研究图的自同构群的本原性也是有意义的.

定义 3.16 称无向或有向图 X 为*点本原图*, 如果 $\mathrm{Aut}(X)$ 在 $V(X)$ 上是本原置换群.

事实上，点本原图就是第 XII 章 §4 研究的本原群的轨道图以及若干轨道图的并．这方面已有很多结果．也有人研究自同构群在边集上的作用是本原的图，即所谓*边本原图*，这里不再赘述．

下面再定义几种比弧传递性更强的图的对称性质．为简单计，我们只考虑无向图．

定义 3.17 设 X 是简单无向图，s 是一个正整数．称 X 中 $s+1$ 个顶点的序列 $v_0v_1\cdots v_s$ 为一个 s-弧，如果 $(v_i,v_{i+1})\in E(X)$，$0\le i\le s-1$，并且对 $s\ge 2$ 有 $v_i\ne v_{i+2}$，$0\le i\le s-2$．

称 X 为 *s-弧传递图*，如果 $\mathrm{Aut}(X)$ 在 X 的所有 s-弧上是传递的．称 X 为 *s-传递图*，如果 X 是 s-弧传递的，但不是 $(s+1)$-弧传递的．

在 §1 中我们定义了图的距离函数，下面我们再定义一种比弧传递图对称性更强的图．

定义 3.18 称无向简单图 X 为*距离传递图*，如果对任意两对顶点 u_1,v_1 和 u_2,v_2，只要 $d(u_1,v_1)=d(u_2,v_2)$，就存在 $\alpha\in\mathrm{Aut}(X)$ 使 $u_1^\alpha=u_2$，$v_1^\alpha=v_2$，其中 $d(u,v)$ 是图 X 的距离函数．

还可以定义其它比弧传递图对称性更强的图，如 Cameron 等研究的 n-传递图，Gardiner 等研究的齐性图等．这里不再赘述．自从有限单群分类完成以后，上述具有高对称性的图的理论得到了很大的发展，特别是关于 s-弧传递图和距离传递图，成果极为丰富．由于目前这方面已有专书讲述，还有多篇综述文章，我们不拟作深入讨论．我们只推荐下面的书和文章供大家参考．它们是

(1) N. Biggs, *Algebraic Graph Theory*, 2nd Edition, Cambridge University Press, 1993. Chapters 17–23.

(2) A.E. Brower, A.M. Cohen and A. Neumaier, *Distance Regular Graphs*, Springer-Verlag, Berlin, 1989.

(3) R.M. Weiss, s-transitive graphs, in *Algebraic Methods in Graph Theory*, Colloq. Math. Soc. J. Bolyai, 25, Szeged, 1978; North-Holland, Amsterdam, 1981; 827–847.

(4) A.D. Gardiner, Symmetry conditions in graphs, in *Surveys in Combinatorics* (Ed. B. Bollobas), London Math. Soc. Lecture Note Series 38, 1979; 22–43.

(5) C.E. Praeger, J. Saxl and K. Yokoyama, Distance transitive graph and finite simple groups, *Proc. London Math. Soc.* (3) **55** (1987), 1–21.

在本章的其余部分，我们着重介绍如何由群来构造图以及关于对称图的一般理论. 这些内容目前在书中还不多见. 用群构造图最简单的方法是构造群的 Cayley 图. 这是下节的内容之一.

习 题

1. 证明命题 3.2.

2. 证明例 3.3 中的全部结论.

3. 以 P_n 表长为 n 的路组成的图，以 C_n 表长为 n 的圈组成的图. 试求 $\mathrm{Aut}(P_n)$ 和 $\mathrm{Aut}(C_n)$. 并讨论对于什么样的 n, P_n 是点传递的，边传递的，和弧传递的. 对于 C_n 讨论同样的问题.

4. 令 $X = C_n[2K_1]$, 即 C_n 和 $2K_1$ 的字典式积. 试求 $\mathrm{Aut}(X)$, 并证明 X 是弧传递的.

5. 一个圈 C_n, $n > 2$, 和完全图 K_2 的笛卡儿积 $X_n = C_n \times K_2$ 叫做柱体. 试求 $\mathrm{Aut}(X_n)$, 并证明 X_n 是点传递的. 再证明 X_n 是边传递的和弧传递的当且仅当 $n = 4$. (下页给出了 X_5 和 X_4 的图示.)

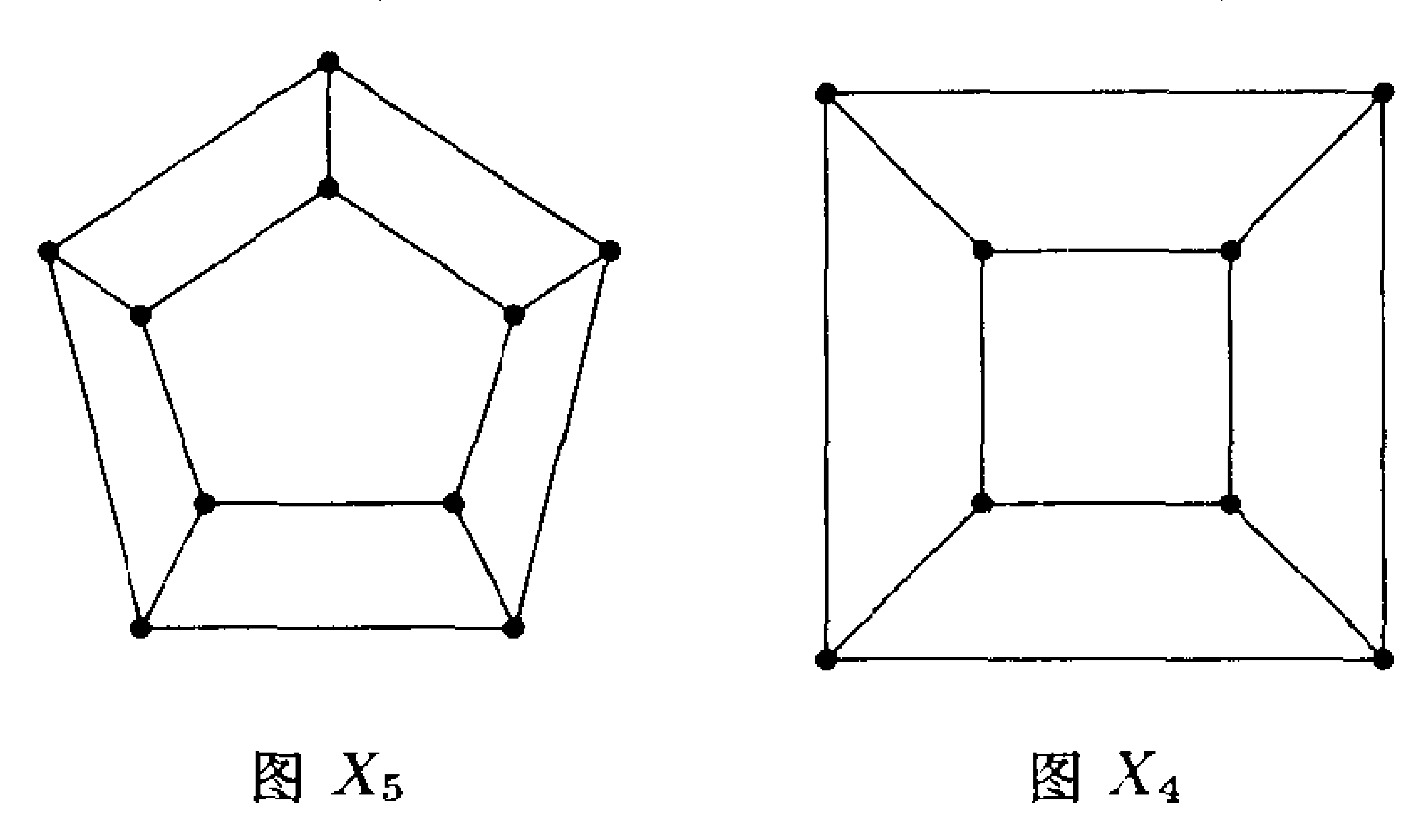


图 X_5 图 X_4

6. 定义 n-立方体 Q_n 如下： $V(Q_n) = \{(c_1, c_2, \cdots, c_n) \mid c_i \in GF(2)\}$, 而两个顶点 $(c_1, c_2, \cdots, c_n)$ 和 $(d_1, d_2, \cdots, d_n)$ 相邻当且仅当存在一个 i 使 $c_i \neq d_i$, 并对所有的 $j \neq i$ 有 $c_j = d_j$. 证明 $Q_n = Q_{n-1} \times K_2$ 且 Q_3 就是上题中定义的 X_4.

7. 设 X 是无向图. 则

(1) X 弧传递当且仅当 X 点传递并且其自同构群在某点的点稳定子群在该点的邻域上的作用传递.

(2) $X \neq mK_2$ 是 2-弧传递的当且仅当 X 点传递并且其自同构群在某点的点稳定子群在该点的邻域上的作用 2 重传递.

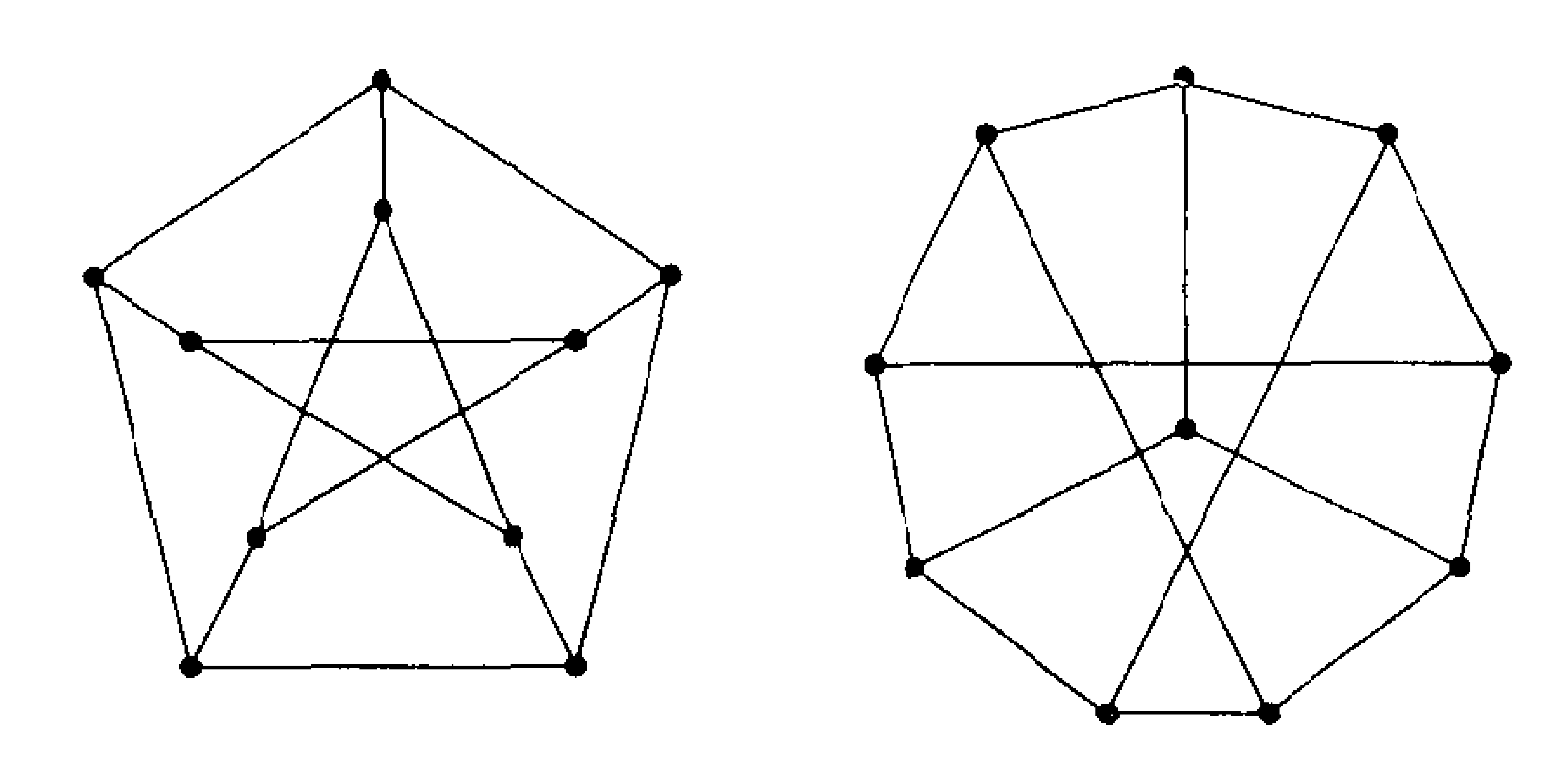
如果 X 是有向图呢?

8. 进一步研究 Q_n 的全自同构群 $\mathrm{Aut}(Q_n)$, 证明 Q_n 是 2-弧传递的.

9. 下图给出了著名的 Petersen 图的两种不同的图示. 试证明

(1) 这两种图示确实代表同一个图.

(2) Petersen 图是 3-弧传递的.



10. 设 $S = \{1, 2, \cdots, n\}$, $n \geq 5$. 设 $\mathcal{B}$ 是 S 的所有二元子集所组成的集合. 定义一个图 X 以 $\mathcal{B}$ 为其顶点集合, 而 $\mathcal{B}$ 中两个顶点 B, C 相邻当且仅当 $B \cap C = \varnothing$. 证明 $\mathrm{Aut}(X)$ 包含 S_n, 且 X 是点传递, 边传递和弧传递的, 并且是点本原的. 对于 $n = 5$ 的情形, X 就是著名的 Petersen 图.

11. 设 V 是 $GF(q)$ 上 n 维向量空间, $n \geq 5$. 设 $\mathcal{B}$ 是 V 的所有二维子空间所组成的集合. 定义一个图 X 以 $\mathcal{B}$ 为其顶点集合, 而 $\mathcal{B}$ 中两个顶点 B, C 相邻当且仅当 $B \cap C = \{0\}$. 证明 $\mathrm{Aut}(X)$ 包含 $P\Gamma L(n, q)$, 且 X 是点传递, 边传递和弧传递的, 并且是点本原的.

(注意在 10, 11 两题中 "$\mathrm{Aut}(X)$ 包含..." 均可改为 "$\mathrm{Aut}(X)$ 等于...", 但证明要求对称群极大子群以及有限几何的知识.)

12. 七点射影平面的点线关联图叫做 Heawood 图. 决定 Heawood 图的全自同构群, 并证明 Heawood 图是 4-弧传递的.

(本题要求有限几何的知识.)

§4. 群的 Cayley 图

Cayley 图由 A. Cayley 在 1878 年提出的, 当时是为了解释群的生成元和定义关系. 但由于它构造的简单性、高度的对称性

和品种的多样性，越来越受到图论学者的重视，成为群与图的一个重要的研究领域. 近二十年来，由于计算机的发展，人们发现 Cayley 图还是构造与设计互连网络的很好的数学原型，因而又获得了实际的应用，它的重要性日益增加. 在本节中我们只来叙述关于它的几个问题. 首先是它的定义.

定义 4.1 设 G 是有限群， S 是 G 的不含单位元的子集，我们如下定义群 G 关于子集 S 的 Cayley (有向) 图 $X = \mathrm{Cay}(G, S)$:

$$\begin{aligned} V(X) &= G, \\ E(X) &= \{(g, sg) \mid g \in G, s \in S\}. \end{aligned}$$

下面的事实是基本的.

命题 4.2 *设 $X = \mathrm{Cay}(G, S)$ 是群 G 关于子集 S 的 Cayley (有向) 图. 则*

(1) $\mathrm{Aut}(X)$ 包含 G 的右正则表示 $R(G)$, (参看 I,§5), 因而 X 是点传递图.

(2) X (作为有向图) 连通当且仅当 X 强连通，当且仅当 $G = \langle S\rangle$.

(3) X 是无向图当且仅当 $S^{-1} = S$, 这里我们把一条无向边 $\{u, v\}$ 等同于两条有向边 (u, v) 和 (v, u).

证 (1) 对于任意的 $x \in G$, 我们要证明 x 对应的右乘变换 $R(x) : g \mapsto gx$, $\forall g \in G$, 是图的自同构. 而这是因为对任意的 $(g, sg) \in E(X)$, $(g, sg)^{R(x)} = (gx, sgx)$ 仍是 X 的边.

(2) X 连通当且仅当对任意的一对顶点 $g, h \in G$, 在 X 的基础无向图中，有一条由 g 到 h 的路. 由 (1), X 是点传递的，故不妨设 $g = 1$. 这样 X 连通就等价于 h 可表成 S 中元素或其逆之积，即 G 可由 S 生成.

最后由 XII, 引理 4.3 得 X 强连通与 X 连通的等价性.

(3) X 无向意味着对任一边 $(g, sg) \in E(X)$, $(sg, g) = (sg, s^{-1}(sg))$ 也是边；而这就等价于若 $s \in S$, 则 $s^{-1} \in S$, 即 $S = S^{-1}$. □

命题 4.3 (有向) 图 $X=(V,E)$ 同构于群 G 的 Cayley (有向) 图当且仅当 $\mathrm{Aut}(X)$ 包含一个同构于 G 的正则子群.

证 由命题 4.2(1) 只须证充分性.

设 $\mathrm{Aut}(X)$ 有正则子群 G, 我们要证 X 同构于 G 的 Cayley 图. 取定一点 $v\in V$. 因 G 在 V 上正则, 对任意的 $u\in V$, 有唯一的 $g\in G$ 使 $u=v^g$. 这样 $u\mapsto g$ 就建立了一个 V 到 G 上的一一映射. 令 $X_1(v)$ 为 v 的出邻域, 即 $X_1(v)=\{u\in V \mid (v,u)\in E\}$. 再令

$$S=\{g\in G \mid v^g\in X_1(v)\}.$$

作 Cayley 图 $Y=\mathrm{Cay}(G,S)$. 我们可以验证前面建立的映射 $u\mapsto g$ 就是图 X 到 Y 的同构. 设 $(u,w)\in E(X)$, $u=v^g$, $w=v^h$. 于是 $(v,v^{hg^{-1}})\in E(X)$. 即 $hg^{-1}\in S$. 由 Cayley 图的定义有 $(g,h)\in E(Y)$, 证毕. □

命题 4.2 告诉我们, 每个 Cayley 图都是点传递图, 但反过来不对. 最简单的例子是 Petersen 图, 参看本书上册附录中的研究题 30(5).

习 题

1. 证明 6 阶点传递图必为循环群 Z_6 的 Cayley 图.
2. 设 p 是素数. 证明 p 阶点传递图必为 Cayley 图.
3. 设 p 是素数. 证明 p^2 阶点传递图必为 Cayley 图.

§4.1 Cayley 图的同构问题

本节研究 Cayley (有向) 图的同构问题. 一般来说, 这个问题是十分复杂的. 首先, 要探索同一个群的不同 Cayley 图之间何时同构; 其次, 不同的群的 Cayley 图之间也可能有同构的情形. (一个极端的例子是 n 点完全图 K_n 是任一 n 阶群的 Cayley 图). 到目前为止, 人们的研究多局限在前一个问题上, 而且多限于研究所谓的 CI 性质. 在引进一些相关的概念之前, 我们先作下面的观察.

设 $X = \mathrm{Cay}(G,S)$ 是群 G 关于子集 S 的 Cayley 有向图. 设 $\alpha \in \mathrm{Aut}(G)$. 则容易验证 α 是由 $\mathrm{Cay}(G,S)$ 到 $\mathrm{Cay}(G,S^\alpha)$ 的图同构. 群 G 的 Cayley 有向图之间的这类同构是由群 G 的自同构诱导出来的, 我们称之为平凡同构. 子集 S 被称为是群 G 的一个 CI-子集 ("CI" 代表 "Cayley invariant"), 如果只要 $\mathrm{Cay}(G,T)$ 同构于 $\mathrm{Cay}(G,S)$, 则这种同构必为平凡同构. 更精确的, 我们有下面的定义.

定义 4.4 (1) 设 G 是有限群, S 是 G 的不包含单位元素的子集. 称 S 为 G 的 CI-子集, (并称 $\mathrm{Cay}(G,S)$ 为 G 的 CI-图), 如果对任意的同构 $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$, 存在 $\alpha \in \mathrm{Aut}(G)$ 使得 $S^\alpha = T$.

(2) 称 G 为 DCI-群, 如果 G 的每个不包含单位元素的子集都是 CI-子集.

(3) 称 G 为 CI-群, 如果 G 的每个满足 $S^{-1} = S$ 的不包含单位元素的子集 S 都是 CI-子集.

(注意在上述定义中, 要求 S 不包含单位元素这点对研究同构问题来说是不重要的. 这个要求只是因为通常我们不考虑有自环的图).

历史上对 Cayley 图同构问题的研究起源于 1967 年 Ádám 提出的一个猜想: 每个有限循环群都是 DCI-群. 尽管这个猜想在 1970 年就被否定, 但它毕竟是近三十年来对 CI-群和 DCI-群探索的起点. 今天我们知道, CI-群和 DCI-群是很稀少的. 对于循环群来说, 8 阶循环群已经不是 DCI-群, 而 16 阶循环群也不是 CI-群. 如果用加法记号, 设循环群 $Z_n = \{0,1,\cdots,n-1\}$. 对于 Z_8 而言, 取 $S = \{1,2,5\}$, $T = \{1,5,6\}$, 则 $\mathrm{Cay}(Z_8,S) \cong \mathrm{Cay}(Z_8,T)$, 但不存在 $\alpha \in \mathrm{Aut}(Z_8)$ 使 $S^\alpha = T$; 而对于 Z_{16}, 则取 $S = \{1,2,5,11,14,15\}$ 和 $T = \{1,2,7,9,14,15\}$. 请读者自行验证.

关于 Ádám 猜想的正面结果也有很多, 譬如在 1970 年证明了对于素数 p, Z_p 是 DCI-群, 后来又证明了 Z_{pq} (其中 q 也是素数), Z_{4p} 也是 DCI-群等等. 事实上, 对于什么样的循环群是 CI-群

的问题，今天我们已经完全解决. 见下面的定理.

定理 4.5 设 $n > 1$ 是正整数. 则 Z_n 是 CI-群当且仅当下述之一成立:

(1) $n = 2^\alpha m$, 其中 $\alpha = 0, 1, 2$ 且 m 无平方因子的奇数.

(2) $n = 8$, 9 或 18.

这个定理第一部分的证明可见下面的文章，而第二部分是根据 B.D. McKay 的计算机搜索的结果.

(1) M. Muzychuk, Ádám's conjecture is true in the square-free case, *J. Combin. Theory (A)* **72** (1995), 118–134.

(2) M. Muzychuk, On Ádám's conjecture for circulant graphs, *Disc. Math.* **167/168** (1997), 497–510.

除了定理 4.5 列出的循环群之外，今天我们还只证明了以下这些群是 CI-群: 初等交换 p-群 Z_p^2, Z_p^3, 四元数群 Q_8, 交错群 A_4, 二面体群 D_{2p}, 其中 p 是素数. 另外， G. Royle 在 1987 年， M. Conder 在 1997 到 1998 年，用计算机搜寻又找到了一些阶较小的 CI-群. Royle 决定了所有阶 ≤ 31 的 CI-群，除了上面已给出的之外，还有 $Z_6 \times Z_2$, Q_{12}, Z_2^4, D_{18}, $Z_6 \times Z_3$, $Z_3^2 \rtimes Z_2$, $Z_6 \times Z_2^2$, $Q_8 \times Z_3$, $Z_3 \rtimes Z_8$, $Z_{14} \times Z_2$, Q_{28}, $D_{10} \times Z_3$, $D_6 \times Z_5$ 和 D_{30}. 而 Conder 又定出了 Z_2^5, $Z_9 \times Z_4$ 以及 $Z_2^2 \times Z_9$ 也是 CI-群. 据我所知，这就是目前所知的全部 CI-群. 但是，如果读者想继续研究 CI-群和 DCI-群，必须首先了解现在的研究现状，避免重复工作.

还值得提出的是，李才恒和 Praeger 得到了有限 CI-群的必要条件，他们证明了

定理 4.6 设 G 是 CI-群. 则 G 的每个 Sylow 子群是初等交换群，或同构于 Z_4, Z_8, Z_9 或 Q_8. 更进一步， $G = U \times V$, 其中 $(|U|, |V|) = 1$, U 是交换群，而 $V = 1$ 或 V 是下列群之一:

(i) Q_8, $Z_2^2 \rtimes Z_3$, $Z_2^2 \rtimes Z_9$, $Q_8 \rtimes Z_3$, $Q_8 \rtimes Z_9$, $Z_3^2 \rtimes Q_8$;

(ii) 一个齐次循环群 M 和另一群 Z 的半直积，其中 $(6, |M|) = 1$, 且 Z 循环，满足 $|Z| = 2^r 3^s$, 或者 $Z = Q_8 \times Z_{3^r}$, 其中 r 和 s 是非负整数.

特别地，CI-群都是可解群.

证明可见李才恒的博士论文：

Cai-Heng Li, *Isomorphisms of Finite Cayley Graphs*, Ph D Thesis at University of Western Australia, 1997.

至此，对于 CI-群和 DCI-群剩下的工作就是回答下面的十分困难的问题.

问题 4.7 定理 4.6 中列出的群中哪些真正是 CI-群？又，哪些 CI-群是 DCI-群？

从上面两个定理可以看出，CI-群是十分稀少的. 因此，为了研究有限群 (不一定是 CI-群) 的 Cayley 图的同构问题，我们应该着重研究下面的问题：

(1) 有限群 G 的什么样的子集是 CI-子集？特别是什么样的生成子集是 CI-子集？(因为我们可只考虑连通的 Cayley 图).

(2) 如果子集 S 不是 G 的 CI-子集，如何刻划满足条件 $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ 的子集 T.

对于上面第二个问题的研究还很少结果，我们不在这里讲述. 而对于第一个问题的研究主要集中在两个方面. 其一是研究小度数的情形，其二是研究极小生成系的情形. 在分别叙述这两个问题之前，我们先给出一个 CI-子集的群论刻划.

定理 4.8 (Babai) 设 G 是有限群，S 是 G 的不包含单位元素的子集. 设 $X = \mathrm{Cay}(G,S)$, $A = \mathrm{Aut}(X)$. 则 S 是 G 的 CI-子集当且仅当对任意的 $\sigma \in S_G$, 这里 S_G 表示 G 上的对称群，满足 $\sigma R(G)\sigma^{-1} \leq A$, 必存在 $a \in A$ 使得 $aR(G)a^{-1} = \sigma R(G)\sigma^{-1}$.

证 $\Longrightarrow$: 假设 S 是 CI-子集. 又假设 $\sigma \in S_G$ 满足 $\sigma R(G)\sigma^{-1} \leq A$, (不失普遍性还可设 $1^\sigma = 1$). 我们要证明存在 $a \in \mathrm{Aut}(X)$ 使得 $aR(G)a^{-1} = \sigma R(G)\sigma^{-1}$.

用 X^σ 表具有顶点集合 G 和边集合 $\{(g^\sigma,(sg)^\sigma) \mid g \in G, s \in S\}$ 的有向图. 容易验证 $\mathrm{Aut}(X^\sigma) = \sigma^{-1}A\sigma$. 于是 $\mathrm{Aut}(X^\sigma) \geq \sigma^{-1}R(G)\sigma$, 这推出 X^σ 也是 G 的 Cayley 图. 因为在图 X^σ 中点

1 的邻域是 S^σ, 我们有 $X^\sigma = \text{Cay}(G, S^\sigma)$. 由 S 是 CI-子集, 存在 $\alpha \in \text{Aut}(G)$ 使 $S^\alpha = S^\sigma$, 于是 $S^{\sigma\alpha^{-1}} = S$. 令 $a = \sigma\alpha^{-1}$, 有 $a \in \text{Aut}(X)$. 又因 α 正规化 $R(G)$, 就得到

$$aR(G)a^{-1} = \sigma\alpha^{-1}R(G)\alpha\sigma^{-1} = \sigma R(G)\sigma^{-1}.$$

$\Longleftarrow$: 设定理条件成立, 又设 σ 是 Cayley 图 $X = \text{Cay}(G, S)$ 到另一 Cayley 图 $Y = \text{Cay}(G, T)$ 的同构, 并设 $1^\sigma = 1$. 我们要证明存在 $\alpha \in \text{Aut}(G)$ 使得 $S^\alpha = T$. 首先有 $S^\sigma = T$ 和 $Y = X^\sigma$. 于是 $\text{Aut}(Y) \geq R(G)$, 这推出 $R(G)$ 和 $\sigma R(G)\sigma^{-1}$ 都包含于 $\text{Aut}(X) = A$. 由定理假设存在 $a \in A$ 使得 $\sigma R(G)\sigma^{-1} = aR(G)a^{-1}$, 这里我们也可假定 $1^a = 1$. 令 $\alpha = a^{-1}\sigma$, 我们有 α 正规化 $R(G)$ 并且 $1^\alpha = 1$. 这推出 $\alpha \in \text{Aut}(G)$ 并且 $S^\alpha = S^{a^{-1}\sigma} = S^\sigma = T$. □

由这个定理, Z_p 是 DCI-群可由有限群的 Sylow p-子群的共轭性推出. 因为 Z_p 的任一 Cayley 图的自同构群都是 p 级传递置换群, 它的正则子群恰为 Sylow p-子群. 类似地, 我们可以证明

定理 4.9 *设 G 是有限 p-群, S 是 G 的包含 d 个元素的生成子集, 且 $d < p$. 设 $X = \text{Cay}(G, S)$. 则 X 是 CI-图, (或 S 是 CI-子集).*

证 设 $A = \text{Aut}(X)$. 如果我们能证明 G 是 A 的 Sylow 子群, 由定理 4.8 即可得到 X 和 S 的 CI-性. 为此我们又只须证明 A 对于 1 的点稳定子群 A_1 的阶与 p 互素.

用反证法, 假定 $p \mid |A_1|$, 并且 α 是 A_1 中的一个 p 阶元素. 因为 $d < p$, 如果 α 不动某点 v, 则必然不动 v 的邻域 Sv 中的每个点. 我们要证明 α 不动图 X 中的任意点, 从而得到矛盾. 因为 S 生成 G, 对任意的 $g \in G$, g 可表成有限个 S 中元素或其逆之积. 又因 G 是有限群, g 甚至可以表成 S 中元素之积. 设 $g = s_n s_{n-1} \cdots s_2 s_1$. 因 $\alpha \in A_1$, 则 α 不动 1, 从而不动 1 的邻域 S 中的每个点, 所以不动 s_1. 同理 α 又不动 s_1 的邻域 Ss_1 中的每个点, 于是 α 不动 $s_2 s_1$. 继续做下去, 即可得到 α 不动 g, 证毕. □

定义 4.10 设 m 是正整数. 群 G 称为 m-DCI-群(或 m-CI-群), 如果 G 的任一势 $\leq m$ 的子集 S (或任一满足 $S^{-1}=S$ 的势 $\leq m$ 的子集) 都是 CI-子集.

关于 m-DCI-群和 m-CI-群的研究是从交换群开始的. 所用的方法主要是组合方法, 典型的结果如下述定理.

定理 4.11 *设 G 是有限交换群. 则*

(1) G 是 1-DCI-群当且仅当它的每个 Sylow 子群是齐次循环群. (齐次循环 p-群指的是若干个同阶循环 p-群的直积.)

(2) G 是 2-DCI-群当且仅当 G 是 1-DCI-群并且它的 Sylow 2-子群 G_2 是循环群或初等交换群.

(3) G 是 3-DCI-群当且仅当对 $p>3$, G 的 Sylow p-子群 G_p 是齐次循环群, 而 G_3 是循环群或初等交换群, G_2 是初等交换群或 $G_2 \cong Z_4$.

(4) G 是 1-CI-群当且仅当它的 Sylow 2-子群 G_2 是齐次循环群.

(5) G 是 m-CI-群, $2 \leq m \leq 5$, 当且仅当 G 是 2-DCI-群, 即它的每个 Sylow 子群是齐次循环群且 G_2 是循环群或初等交换群.

这个定理的证明可见下列文章及其后所附的文献.

Fang Xingui(方新贵) and Xu Mingyao(徐明曜), On isomorphisms of Cayley graphs of small valency, *Algebra Colloq.*, **1** (1994), 67–76.

如果我们不只限于考虑交换群, 对于 m-DCI-群和 m-CI-群的研究将产生很多有趣的群论问题. 首先, 容易看出群 G 是 1-DCI-群当且仅当群 G 的自同构群 $\mathrm{Aut}(G)$ 在群 G 的同阶元素的集合上是传递的, 我们把这种群叫做 T-群. 对 G 是 p-群的情形, 在六十年代研究的所谓 p-自同构 p-群 (只要求自同构群在群的 p 阶元素的集合上是传递的) 在 $p>2$ 时和 T-群是等价的. 这时我们能够推出这样的群必然是交换群, 并且是齐次循环群. 对于 $p=2$ 的情形则比较复杂. 这时无论是 T-群还是 2-自同构 2-群都不一

定是交换的，比如 8 阶四元数群 Q_8 就是一例. 最近，决定非交换的 2-自同构 2-群这个长期悬而未决的问题已被 Wilkens 解决，从而非交换的 T-2-群也被完全决定. 对于前者，它们就是 Q_8 和所谓的 Suzuki 2-群 (Suzuki 2-群可参看 Huppert 和 Blackburn 的 "Finite Groups" 卷 II, 第 VII 章 §7); 而对于后者，则是 Q_8 和满足条件 $|G| = |Z(G)|^2$ 的 Suzuki 2-群 G.

关于 T-群的其它结果有： Gaschütz 和 Yen 首先证明了对于奇素数 p, p-可解 T-群的 p-长为 1. 张继平则得到了 T-群的一个分类，而 Praeger, 李才恒和徐明曜又得到了 T-群的更精细的结构. 以上所述结果可参看下列文章.

(1) E.E. Shult, On finite automorphic algebras, *Illinois J. Math.* **13** (1969), 625-653.

(2) F. Gross, 2-automorphic 2-groups, *J. Algebra* **40** (1976), 348-353.

(3) B. Wilkens, A note on 2-automorphic 2-groups, *J. Algebra*, **184**(1996), 199–206.

(4) W. Gaschütz and T. Yen, Groups with an automorphism group which is transitive on the elements of prime order, *Math. Z.* **86** (1964), 123-127.

(5) J.P. Zhang, On finite groups all of whose elements of the same order are conjugate in their automorphism groups, *J. Algebra*, **153** (1992) 22-36.

(6) Cai Heng Li, Cheryl E. Praeger and Ming Yao Xu, Isomorphisms of finite Cayley digraphs of bounded valency, *J. Combin. Theory Ser. B*, **73**(1998), 164–183.

在研究 m-DCI-群时碰到的另一群论问题是所谓 *齐次群* 的决定.

定义 4.12 有限群 G 称为是 *齐次群*, 如果给定它的任二同构的子群 H 和 K, 以及它们之间的任一同构 $\sigma : H \to K$, 则 σ 可扩展成为 G 的一个自同构 α.

明显的，齐次群必为 1-DCI 群．而且，对于交换群的情形，二者是等价的．我们有下面的

定理 4.13 有限交换群 G 是齐次群当且仅当 G 是 1-DCI-群，即对任意的素数 p, G 的 Sylow p-子群是齐次循环群.

首先我们证明一个引理.

引理 4.14 有限交换 p-群 G 是齐次的当且仅当 G 是齐次循环群.

证 $\Longrightarrow$: 设 $\exp G = p^e$. 若 G 不是齐次循环的，则 $\Omega_1(G) > \mho_{e-1}(G)$, 且这两个子群都是 G 的特征子群．取子群 $M \le \Omega_1(G)$ 满足 $|M| = |\mho_{e-1}(G)|$ 但 $M \neq \mho_{e-1}(G)$. ($\Omega_i(G)$ 和 $\mho_j(G)$ 的定义可见第 X 章 §2.) 我们有 $M \cong \mho_{e-1}(G)$, 但由 M 到 $\mho_{e-1}(G)$ 上的任何同构都不能扩展为 G 的自同构，与 G 是齐次群相矛盾.

$\Longleftarrow$: 设 G 是齐次循环群且 $\exp G = p^e$, 又设 H 和 K 是 G 的同构子群且 σ 是由 H 到 K 上的同构．我们要找 $\alpha \in \mathrm{Aut}(G)$ 使 $\alpha|_H = \sigma$.

首先我们注意到下述事实.

(1) 对任意的 $x \in G$, 存在元素 a 使得 $o(a) = p^e$ 且对某个 i 有 $x = a^{p^i}$.

(2) 对 G 的任一方次数为 p^e 的齐次循环真子群 C, 存在一方次数为 p^e 的子群 D 使得 $G = C \times D$. (证明之 !)

(3) G 的任一自同构 α 把一组基仍变到一组基. 并且反过来，给定 G 的两组基 $(a_1, a_2, \cdots, a_s)$ 和 $(b_1, b_2, \cdots, b_s)$, 则存在 $\alpha \in \mathrm{Aut}(G)$ 使对所有 i 有 $a_i^\alpha = b_i^\alpha$.

现在取 H 的一组基 $(x_1, x_2, \cdots, x_t)$. 假定 $y_i = x_i^\sigma$, $\forall i$. 则 $(y_1, y_2, \cdots, y_t)$ 是 K 的一组基．由 (1), 对任意的 i 存在 $c_i \in G$ 使得 $o(c_i) = p^e$ 并且 x_i 是 c_i 的方幂，譬如 $c_i^{p^{e_i}} = x_i$. 同理存在 $d_i \in G$ 使得 $o(d_i) = p^e$ 并且 $d_i^{p^{e_i}} = y_i$. 记 $C = \langle c_1, c_2, \cdots, c_t \rangle$, $D = \langle d_1, d_2, \cdots, d_t \rangle$. 则 C 和 D 是方次数为 p^e 的齐次循环群，并且 $(c_1, c_2, \cdots, c_t)$ 和 $(d_1, d_2, \cdots, d_t)$ 分别是 C 和 D 的一组基. 由 (2) 它

们可分别扩充为 G 的基 $(c_1, c_2, \cdots, c_t, \cdots, c_s)$ 和 $(d_1, d_2, \cdots, d_t, \cdots, d_s)$. 最后由 (3) 我们可找到 G 的自同构 α 把 c_i 映到 d_i. 这样，α 是 σ 的扩张. 引理证毕. □

定理 4.13 **的证明**: $\Longrightarrow$: 假设 G 是齐次群. 因齐次群的每个特征子群也是齐次群，故 G 的每个 Sylow 子群是齐次循环群.

$\Longleftarrow$: 假定 $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}$, 其中 G_{p_i} 是 G 的 Sylow p_i-子群，并且它是方次数为 p^{e_i} 的齐次循环群. 假定 H 和 K 是 G 的两个同构的子群，且 σ 是由 H 到 K 上的同构. 我们要找 $\alpha \in \mathrm{Aut}(G)$, 使得 $\alpha|_H = \sigma$.

记 $H = H_1 \times H_2 \times \cdots \times H_k$, $K = K_1 \times K_2 \times \cdots \times K_k$, 其中 H_i 和 K_i 分别是 H 和 K 的 Sylow p_i-子群. 则 H_i 和 K_i 是 G_{p_i} 的同构的子群. 令 $\sigma_i = \sigma|_{H_i}$. 则 σ_i 是由 H_i 到 K_i 上的同构. 由引理 4.14, 存在 $\alpha_i \in \mathrm{Aut}(G_{p_i})$ 使得 $\alpha_i|_{H_i} = \sigma_i$. 令 $\alpha = \alpha_1\alpha_2\cdots\alpha_k$. 则 $\alpha \in \mathrm{Aut}(G)$ 且 $\alpha|_H = \sigma$. 定理证毕. □

对于非交换的齐次群还未完全决定，这是个值得进一步研究的问题.

另外，在对较小的 m 研究 m-CI-群时也将碰到一些群论问题. 由定义容易看出，有限群 G 是 1-CI-群当且仅当 G 的所有对合在 Aut(G) 下共轭. 又，若 G 是 2-CI-群，则对 G 的任二同阶元素 x, y, 存在 $\alpha \in \mathrm{Aut}(G)$ 使 $x^\alpha = y$ 或 $x^\alpha = y^{-1}$. 满足上述条件的群叫做 FIF-群. 李才恒和 Praeger 系统研究了 FIF-群，对于它们的构造给了很好的描述，可见下列二文:

(1) C.H. Li and C.E. Praeger, The finite simple groups with at most two fusion classes of every order, *Comm. Algebra* **24(11)** (1996), 3681-3704.

(2) C.H. Li and C.E. Praeger, Finite groups in which any two elements of the same order are either fused or inverse-fused, *Comm. Algebra*, **25** (1997), 3081–3118.

回到 m-DCI-群和 m-CI-群的研究，我们现在已经得到它们的很多必要条件. 作为例子，对于 2-DCI-群，下列定理给出了它们

的一个明确的分类. 但是定理中所列的群是否确系 2-DCI-群, 还需要进一步的研究.

为叙述定理, 我们称有限交换群为齐次循环的, 如果它的每个 Sylow p-子群都是齐次循环 p-群.

定理 4.15 设 G 是 2-DCI-群. 则 $G = U \times V$, 满足 $(|U|, |V|) = 1$, 并且 U 是奇数阶齐次循环交换群, 而 $V = 1$ 或 V 是下列群之一:

(i) Z_2^d, Z_{2^d}, $d \geq 1$.

(ii) Q_8, A_4, $Q_8 \rtimes Z_3$, $Z_3^2 \rtimes Q_8$ 和 A_5;

(iii) 奇数阶齐次循环群 M 和循环 2-群 $Z = \langle z \rangle$ 的半直积, 且对任意的 $g \in M$, $g^z = g^{-1}$.

如果 G 是 m-DCI-群, $m \geq 3$, 则 G 的结构还有更进一步的限制. 关于以上定理的证明以及关于 m-DCI-群的更进一步的结果可见下列文章:

Cai Heng Li, Cheryl E. Praeger and Ming Yao Xu, Isomorphisms of finite Cayley digraphs of bounded valency, *J. Combin. Theory Ser. B*, **73**(1998), 164–183.

对于 m-CI-群也有类似的结果, 但限于篇幅, 我们不在这里讲述. 另一方面, 为了研究在定理 4.15 以及在上述文章中其它类似定理中列出的群是否真是 2-DCI-群 (或 m-DCI-群), 我们建议研究下列问题.

问题 4.16 设 U 和 V 都是 m-DCI-群, $m \geq 2$. 令 $G = U \times V$. 如果 $(|U|, |V|) = 1$, 问 G 是否也是 m-DCI-群?

类似于 m-DCI-群和 m-CI-群, 为研究连通 Cayley 图的同构问题, 我们有下面的定义.

定义 4.17 设 m 是正整数. 群 G 称为*弱 m-DCI-群*(或*弱 m-CI-群*), 如果 G 的任一势 $\leq m$ 的生成子集 S (或任一满足 $S^{-1} = S$ 的势 $\leq m$ 的生成子集) 都是 CI-子集.

表面看来，这个定义和定义 4.10 差别不大，但实质上是很不相同的. 例如，定理 4.9 说明，对奇素数 p, 任意二元生成的有限 p-群都是弱 2-DCI-群，可是 1-DCI 性就迫使该有限 p-群必为齐次循环群.

关于弱 m-DCI-群和弱 m-CI-群的结果现在还不多. 目前已发表的关于连通 Cayley 图的同构问题的文章一般都是关于下面的问题的.

问题 4.18 设 G 是有限群而 S 是 G 的一个极小生成系. 问: 是否 S 和 $S\cup S^{-1}$ 一定是 G 的 CI-子集?

关于这个问题的研究还在进行当中，有兴趣的读者可参看下列文章.

Ming-Yao Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.*, **182** (1998), 309–319.

习 题

4. 设 $|G|=n, m<n-1$. 则 G 是 m-DCI-群当且仅当 G 是 $(n-m-1)$-DCI-群.
5. 证明二面体群 D_6 是 DCI-群.
6. 证明四元数群 Q_8 是 DCI-群.
7. 证明对任意的正整数 n, 循环群 Z_n 是 2-DCI-群.
8. 设 $n\geq 5$, $n\neq 6$, 则循环群 Z_{n^2} 不是 CI-群.
9. 证明 $2p$ 阶群都是 DCI-群, 其中 p 为素数.

§4.2 Cayley 图的自同构群

设 G 是有限群， $S\subseteq G$, $X=\mathrm{Cay}(G,S)$. 设 $A=\mathrm{Aut}(X)$ 是图 X 的全自同构群. 由命题 4.2 知 $\mathrm{Aut}(X)\geq R(G)$. 但一般来说，可能有 $\mathrm{Aut}(X)>R(G)$. 事实上，决定一个图的全自同构群是十分困难的. 本小节只介绍两个关于这方面的问题.

第一个是 70 年代人们研究的有限群的图正则表示的问题.

定义 4.19 设 G 是有限群. 称 (无向) 图 X 为 G 的**图正则表示** (GRR), 如果 X 的自同构群 $\mathrm{Aut}(X)$ 同构于 G, 并且在 $V(X)$ 上

作用正则. 而称 (有向) 图 Y 为 G 的有向图正则表示 (DRR), 如果 Y 的自同构群 $\mathrm{Aut}(Y)$ 同构于 G, 并且在 $V(Y)$ 上作用正则.

称群 G 为广义双循环群, 如果 G 有一个指数为 2 的交换子群 A 和一个 4 阶元素 $b \in G \setminus A$ 使得 $a^b = a^{-1}$, $\forall a \in A$.

关于 GRR 问题和 DRR 问题的主要结果是下面的两个定理.

定理 4.20 除了下列三类群之外, 每个有限群都有一个 GRR:

类 C: 方次数大于 2 的交换群.

类 D: 广义双循环群.

类 E: 下列十三个 "例外群":

(1) Z_2^2, Z_2^3, Z_2^4.

(2) D_6, D_8, D_{10}.

(3) A_4.

(4) $\langle a, b, c \mid a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle$.

(5) $\langle a, b \mid a^8 = b^2 = 1, bab = b^5 \rangle$.

(6) $\langle a, b, c \mid a^3 = c^3 = b^2 = 1, ac = ca, (ab)^2 = (cb)^2 = 1 \rangle$.

(7) $\langle a, b, c \mid a^3 = b^3 = c^3 = 1, ac = ca, bc = cb, c = a^{-1}b^{-1}ab \rangle$.

(8) $Q_8 \times Z_3$, $Q_8 \times Z_4$.

定理 4.21 除了五个例外, 每个有限群都有一个 DRR. 这五个例外是 4, 8, 9, 16 阶初等交换群和 8 阶四元数群 Q_8.

以上两个定理的证明可见下列文章:

C. D. Godsil, Neighbourhoods of transitive graphs anf GRR's, *J. Combin. Theory Ser. B* **29**(1980), 116-140.

C. D. Godsil, GRR's for non-solvable groups, in *Algebraic Methods in Graph Theory*, Colloq. Math. Soc. J. Bolyai, 25. Szeged, 1978; North-Holland, Amsterdam, 1981; 221-239.

L. Babai, Finite digraphs with given regular automorphism groups, *Periodica Math Hung*, **11**(1980), 257–270.

第二个问题是所谓正规 Cayley 图的问题. 首先我们有下面的观察.

设 $X = \mathrm{Cay}(G,S)$ 是有限群 G 关于子集 S 的 Cayley 图. 设 $A = \mathrm{Aut}(X)$. 由命题 4.2 有 $A \geq R(G)$. 又设 $\mathrm{Aut}(G,S) = \{\alpha \in \mathrm{Aut}(G) \mid S^\alpha = S\}$. 显然也有 $A \geq \mathrm{Aut}(G,S)$. 于是 $A \geq R(G)\mathrm{Aut}(G,S)$. 进一步有

命题 4.22 (1) $N_A(R(G)) = R(G)\mathrm{Aut}(G,S)$;

(2) $A = R(G)\mathrm{Aut}(G,S)$ 等价于 $R(G) \trianglelefteq A$.

证 因为 $R(G)$ 在 G 上的对称群 S_G 中的正规化子是 G 的全形, 即 $R(G)\mathrm{Aut}(G)$, 我们有 $N_A(R(G)) = R(G)\mathrm{Aut}(G) \cap A = R(G)\mathrm{Aut}(G) \cap R(G)A_1 = R(G)(\mathrm{Aut}(G) \cap A_1)$, 其中 A_1 是单位元素 1 在 A 中的点稳定子群.

显然, $\mathrm{Aut}(G) \cap A_1 = \mathrm{Aut}(G,S)$. 于是 (1) 成立.

(2) 是 (1) 的直接推论. □

定义 4.23 Cayley (有向) 图 $X = \mathrm{Cay}(G,S)$ 叫做 *正规的*, 如果 $R(G) \lhd A = \mathrm{Aut}(X)$.

由命题 4.22 和上定义可知, 正规 Cayley 图具有最小可能的自同构群, 即满足 $\mathrm{Aut}(X) = R(G)\mathrm{Aut}(G,S)$. 显然, 有限群的 GRR 和 DRR 都是正规的. 并且我们有

命题 4.24 *设 $X = \mathrm{Cay}(G,S)$ 是群 G 关于子集 S 的 Cayley (有向) 图, $A = \mathrm{Aut}(X)$. 设 A_1 是单位元 1 在 A 中的稳定子群. 则 X 正规当且仅当 A_1 的每个元素都是群 G 的自同构.*

应该注意, Cayley 图是否正规是依赖于群 G 的. 例如, 完全图 K_4 作为群 $Z_2 \times Z_2$ 的 Cayley 图是正规的, 但作为群 Z_4 的 Cayley 图则不正规.

关于 Cayley (有向) 图正规性的研究目前还刚刚开始, 我们只想介绍下面的几个结果和几个需要进一步研究的问题. 和定理 4.20 和 4.21 类似, 我们有

定理 4.25 (1) *每个有限群都至少有一个正规的 Cayley 有向图.*

(2) 除了 $Z_4 \times Z_2$ 和 $Q_8 \times Z_2^m$ $(m \geq 0)$ 之外, 每个有限群都至少有一个正规的 Cayley 图.

以上定理的证明可见下列文章:

王长群, 王殿军, 徐明曜, 有限群的正规 Cayley 图, 中国科学, **28**(1998), 131–139.

对于 $n \geq 5$, 完全图 K_n 和它的补 nK_1 的全自同构群是 S_n, 它们作为任一 n 阶群的 Cayley 图显然都是非正规的. 对于素数阶循环群来说, 我们有

例 4.26 设 $G = Z_p, p \geq 5$ 是素数. 则 G 的所有 Cayley 有向图, 除了 K_p 和 pK_1 外, 都是正规的.

第一个值得研究的问题, 也是比较基本的问题是: 对于某个或某类指定的有限群, 决定何时它的或它们的 Cayley 图是正规的, 何时是非正规的. 这个问题对 $2p$ 阶群 (p 是素数) 已经解决, 对其它群结果还不多见.

对于交换群的小度数 Cayley 图, 我们有

定理 4.27 设 $X = \mathrm{Cay}(G, S)$ 是有限交换群 G 的度数小于或等于 4 的 Cayley 图. 则除了下列情形外 X 都是正规的.

(1) $G = Z_4$, $S = G \setminus \{1\}$, $X = K_4$.

(2) $G = Z_4 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, b\}$, $X = Q_3$ 是正立方体.

(3) $G = Z_6 = \langle a \rangle$, $S = \{a, a^3, a^5\}$, $X = K_{3,3}$.

(4) $G = Z_2^3 = \langle u \rangle \times \langle v \rangle \times \langle w \rangle$, $S = \{w, wu, wv, wuv\}$, $X = K_{4,4}$.

(5) $G = Z_4 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^2, a^3, b\}$, $X = Q_3^c$ 是正立方体的补图.

(6) $G = Z_4 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, a^2 b, b\}$, $X = K_{4,4}$.

(7) $G = Z_4 \times Z_2^2 = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$, $S = \{a, a^{-1}, b, c\}$, $X = C_4 \times C_4 = Q_4$, 称为 4 维立方体.

(8) $G = Z_5$, $S = G \setminus \{1\}$, $X = K_5$.

(9) $G = Z_4 \times Z_4 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, b, b^{-1}\}$, $X = C_4 \times C_4 = Q_4$.

(10) $G = Z_{10} = \langle a \rangle$, $S = \{a, a^3, a^5, a^7\}$, $X = K_{5,5} - 5K_2$.

(11) $G = Z_6 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, a^3, b\}$, $X = K_{3,3} \times K_2$.

(12) $G = Z_m \times Z_2 = \langle a \rangle \times \langle b \rangle$, $m \geq 3$, $S = \{a, ab, a^{-1}, a^{-1}b\}$, $X = C_m[2K_1]$.

(13) $G = Z_{4m} = \langle a \rangle$, $m \geq 2$, $S = \{a, a^{2m+1}, a^{-1}, a^{2m-1}\}$, $X = C_{2m}[2K_1]$.

推论 4.28 (1) 奇数阶交换群的 4 度连通 Cayley 图中只有 K_5 (对群 Z_5) 是非正规的.

(2) 有限循环群 G 的度数至多为 4 的连通 Cayley 图 X 中，非正规的只有 (i) $G = Z_4$, $X = K_4$; (ii) $G = Z_5$, $X = K_5$; (iii) $G = Z_{10} = \langle a \rangle$, $X = K_{5,5} - 5K_2$; (iv) $G = Z_{2m}$, $X = C_m[2K_1]$ ($m \geq 3$).

以上定理和推论的证明可见下列文章:

Young-Gheel Baik, Yan-Quan Feng, Hyo-Seob Sim and Ming-Yao Xu, On the normality of Cayley graphs of abelian groups, *Algebra Colloq.*, **5**(1998), 297–304.

最后我们提出以下问题.

问题 4.29 (1) 决定所有奇数阶有限群的非正规的 4 度连通 Cayley 图.

(2) 决定有限循环群的非正规连通 Cayley 图. (平凡的例子是完全图和较小的循环群的 Cayley 图, 即循环图的字典式积).

(3) 有限非交换单群的度数最多为 4 的连通 Cayley 图是否都是正规的?

习 题

10. 证明 8 阶初等交换群的任一 Cayley 图的自同构群的阶均大于 8, 从而它没有 GRR.

11. 证明 8 阶四元数群 Q_8 的任一 Cayley 有向图的自同构群的阶均大于 8, 从而它没有 DRR.

12. 证明 $Z_4 \times Z_2$ 的任一 Cayley 图均非正规.

13. 证明例 4.26 的结论.

§4.3 Cayley 图的 Hamilton 性

设 $X = (V, E)$ 是连通图. 称 X 中的圈为 Hamilton 圈, 如果它经过图的每个顶点恰好一次. X 中的路为 Hamilton 路, 如果它经过图的每个顶点恰好一次.

一个图是否具有 Hamilton 圈和 Hamilton 路的问题是图论研究的重要问题之一，它具有重要的理论意义和实际意义. 但在这里我们并不打算一般地来介绍这个问题. 我们只想谈谈关于点传递图和群的 Cayley 图的 Hamilton 圈的问题. 注意这里谈的都是关于无向图的，有向图的情形则有很大的不同.

至今人们只发现了四个没有 Hamilton 圈的连通点传递图，但它们都不是群的 Cayley 图，并且它们都有 Hamilton 路. 于是我们有下面的猜想.

猜想 4.30 (1) *每个连通点传递图都有 Hamilton 路.*

(2) *每个有限群的连通 Cayley 图都有 Hamilton 圈.*

这两个猜想至今仍未得到解决. 对于第一个猜想，我只想提出 Marušič 的工作. 他证明这个猜想对于阶为 $p, 2p, 3p, 4p, 5p, p^2, p^3$ 和 $2p^2$ 的点传递图是正确的. 可参看下列文章及其后所附的文献.

(1) D. Marušič, Hamiltonian cycles in vertex-symmetric graphs of order $2p^2$, *Discrete Math.*, 66(1987), 169–174.

(2) D. Marušič and T.D. Parsons, Hamiltonian paths in vertex-symmetric graphs of order $5p$, *Discrete Math.*, **42** (1982), 227–242.

对于第二个猜想则研究较多. 好的综述文章有

(1) D. Witte and J.A. Gallian, A survey: hamiltonian cycles in Cayley graphs, *Discrete Math.*, **51** (1984), 293–304.

(2) D. Witte, On hamiltonian circuits in Cayley diagrams, *Discrete Math.*, **38** (1982), 99–108.

值得提出的结果有，对于交换群和导群为素数幂阶循环群的有限群猜想是正确的；二面体群的三度连通 Cayley 图有 Hamilton 圈；以及下面的令人感到惊异的结果.

定理 4.31 有限 p-群的每个连通 Cayley 有向图都有有向的 Hamilton 圈.

可见下文：

D. Witte, Cayley diagrams of prime-power order are hamiltonian, *J. Combin. Theory* **40B** (1986), 107–112.

还值得提出的结果是下面的

定理 4.32 设 G 是有限群，S 是 G 的不包含单位元 1 的生成子集，且满足 $S^{-1}=S$. 如果 S 是 G 中若干完整的共轭类的并，则 Cayley 图 $X=\mathrm{Cay}(G,S)$ 有 Hamilton 圈.

这个结果给出了一大批新的具有 Hamilton 圈的 Cayley 图. 可见下文：

Jun Wang and Ming-Yao Xu, Quasi-abelian Cayley graphs and Parsons graphs, *European J. Combin.*, **18** (1997), 597–600.

习　题

14. 证明任一阶 ≥ 3 的交换群的连通 Cayley 无向图都有 Hamilton 圈.

§4.4 Sabidussi 陪集图

前面提到过，群的 Cayley 图一定是点传递图，但点传递图不一定都是群的 Cayley 图. Sabidussi 给出了另一种用群来构造点传递图的方法，叫做 Sabidussi 陪集图. 与 Cayley 图不同的是，每个点传递图都是适当构造的 Sabidussi 陪集图.

定义 4.33 设 G 是有限群，H 是 G 的子群. 设 D 是若干个形如 HgH ($g \notin H$) 的双陪集的并. 我们定义 G 关于 H 和 D 的 Sabidussi 陪集 (有向) 图 $X = \mathrm{Sab}(G, H, D)$ 如下：

$$\begin{aligned} V(X) &= [G:H], \ (H \text{ 在 } G \text{ 中的右陪集的集合}), \\ E(X) &= \{(Hg, Hdg) \mid g \in G, d \in D\}. \end{aligned}$$

注意，因为我们不考虑重图，如果 $Hdg = Hd_1g$, 我们认为边 (Hg, Hdg) 和 (Hg, Hd_1g) 是同一条边.

由此定义我们可看出 Cayley 图是 Sabidussi 陪集图的特殊情形 (对应于 $H = 1$).

下面的命题是基本的，也是容易证明的.

命题 4.34 *设 $X = \mathrm{Sab}(G, H, D)$ 是 G 关于 H 和 D 的 Sabidussi 陪集有向图. 则*

(1) X 是良定义的出度入度均为 $|D:H|$ 的有向图.

(2) $\mathrm{Aut}(X)$ 包含 G (依右乘变换), 于是 X 是点传递图. 又，顶点 Hg 在 G 中的稳定子群是 $g^{-1}Hg$.

(3) X 是连通的当且仅当 $G = \langle D \rangle$.

(4) X 是无向的当且仅当 $D^{-1} = D$.

(5) X 是 G-弧传递的当且仅当 $D = Hg_iH$ 是一个单个的双陪集.

与 Cayley 图不同的是, 任一点传递图都是 Sabidussi 陪集图. 事实上，任给一点传递图 X 和顶点 $v \in V(X)$, 取 $G = \mathrm{Aut}(X)$, $H = G_v$ 以及 $D = \{g \in G \mid v^g \in X_1(v)\}$. 则 D 是形如 HgH 的双陪集的并，且满足 $D \cap H = \varnothing$, 并且这时有 $X \cong \mathrm{Sab}(G, H, D)$. (证明请读者补足.)

习 题

15. 证明命题 4.34.

§5. 对称图的一般理论

自本节起我们只考虑无向简单图. 在本节中我们将对对称图即弧传递图作些一般的讨论.

设 X 是对称图, $A=\mathrm{Aut}(X)$ 是它的自同构群. 由定义, A 在 X 的弧集上的作用是传递的. 或者等价地, A 在 X 的点集 $V(X)$ 上是传递的, 并且任一点 $v\in V(X)$ 在 A 中的稳定子群 A_v 在 v 的邻域 $X_1(v)$ 上也是传递的.

首先我们看对称图的存在性. 这里有两种看法, 或者说两种构造方法. 一个是抽象群的方法, 另一个是置换群的方法. 上节的命题 4.34 给出了抽象群的方法. 它告诉我们, 对于任一有限群 G 和它的一个子群 H, 如果存在一个 H 的双陪集 $D=HgH$ 满足 $D^{-1}=D$, 则由 G,H 和 D 构造出的 Sabidussi 陪集图 $X=\mathrm{Sab}(G,H,D)$ 就是一个 (无向) 对称图. 如果又有 $\langle D\rangle=G$, 则 X 是一个连通对称图. 置换群的构造方法可见第 XII 章 §4. 每个传递置换群的自配对轨道图都是一个无向对称图, 又容易看出, 任一偶阶的传递置换群都至少有一个自配对次轨道. 由此看来, 对称图的存在性是当然的. 并且由于群的多样性, 对称图也是非常之多的. 因此对称图的一般的分类问题是无法解决的, 因而也是没有意义的.

为了分析对称图及其自同构群的构造, 把对称图分为点本原和非点本原两类是合理的.

§5.1 点本原对称图

点本原对称图是本原群的自配对轨道图, 它们的决定实际上是决定本原群的次轨道结构. 因此本原群的分类是决定点本原对称图的前提. 目前本原群的分类尚未完成, 但已经有了很多的本原群的分类定理. 对于某一类已知的本原群, 为了决定以它们为自同构群 (但不一定是全自同构群) 的点本原对称图, 我们首先需要决定它们的次轨道结构. 这一步还没有一般的方法, 通常要根据该本原群的具体构造使用群论的, 几何的和组合的方法. 完成了这一步以后, 要从中选出自配对的那些, 并且逐一研究它们

的全自同构群. 这里又需要本原群之间相互包含以及该本原群在同级的对称群中是否为极大子群的结果. 还要注意, 本原群的互相配对的两个非自配对轨道图的并可能是某个更大的本原群的自配对轨道图. 通过所有这些步骤, 我们将找到所有以某个给定的本原群为自同构群的所有点本原对称图, 并且决定了它们的全自同构群. 由以上的叙述可以看出, 点本原对称图的决定完全是一个群论的问题, 它是本原群理论的一个重要的组成部分. 限于篇幅, 我们不再作进一步的讲述, 只给出一个例子. 即在下文中决定了所有阶为两个不同素数乘积的所有点本原对称图, 而且还包括有向图的情况:

C.E.Praeger and M.Y. Xu, Vertex primitive graphs of order a product of two distinct primes, *J. Combin. Theory Ser. B*, **59** (1993), 245–266.

习 题

1. 令 $\Omega=\{1,2,\cdots,n\}$, $n\geq 5$. 令 $\mathcal{B}$ 为 Ω 的所有二元子集所组成的集合. 则考虑 S_Ω 在 $\mathcal{B}$ 上的自然作用使 S_Ω 成为 $\mathcal{B}$ 上的本原群, 这个本原群记作 G. 试求所有以 G 为自同构群的点本原图.

2. 试求所有的 10 阶点本原图.

§5.2 非点本原对称图

本节我们讨论非点本原的无向对称图. 不失普遍性我们只考虑连通的情形.

设 X 是一个无向连通简单图, $G\leq \mathrm{Aut}(X)$. 我们称 X 为 G-对称的, 如果 G 在 X 的弧集上是传递的. 称 X 为对称的, 如果 $\mathrm{Aut}(X)$ 在 X 的弧集上是传递的. (见定义 3.7.)

设 X 是 G-对称图, 并设 G 在 $V=V(X)$ 上的作用是非本原的. 又设 $\mathcal{B}=\{B_1,B_2,\cdots,B_n\}$ 是 G 的一个非平凡完全块系. 下面我们定义 X 关于 $\mathcal{B}$ 的 **块图** 或 **商图** $\overline{X}$.

定义 5.1 如下规定的图 $\overline{X}$ 称为 X 关于 $\mathcal{B}$ 的块图或商图:

$$V(\overline{X}) = \mathcal{B},$$
$$E(\overline{X}) = \{\{B_i, B_j\} \mid \text{存在 } v_i \in B_i,\ v_j \in B_j \text{ 使得 } \{v_i, v_j\} \in E(X)\}.$$

我们有下面的

引理 5.2 (1) 块图 $\overline{X}$ 也是 G-对称的 (这里考虑 G 在 $\overline{X}$ 上的自然作用);

(2) 块图 $\overline{X}$ 也是连通的;

(3) 对于任意的块 $B \in \mathcal{B}$, B 中不含图 X 的边.

证 (1) 设 $(B_1, B_2), (B_1', B_2')$ 是块图 $\overline{X}$ 的两条弧, 由定义存在 $v_1 \in B_1$, $v_2 \in B_2$, $v_1' \in B_1'$ 和 $v_2' \in B_2'$ 使得 (v_1, v_2) 和 (v_1', v_2') 是图 X 的两条弧. 于是存在 $g \in G$ 使得 $v_1^g = v_1'$, $v_2^g = v_2'$. 这推出 $B_1^g = B_1'$, $B_2^g = B_2'$, 于是 $\overline{X}$ 也是 G-对称的.

(2) 显然.

(3) 设 $u, v \in B$ 且 $\{u, v\} \in E(X)$. 又设 $v' \in X_1(u)$, $X_1(u)$ 为 u 在图 X 中的邻域. 由 X 的 G-对称性, 存在 $g \in G_u$ 使得 $v^g = v'$. 于是 $B^g \cap B \neq \varnothing$, 这推出 $B^g = B$. 这样 $v' \in B$, 并进而 $X_1(u) \subseteq B$. 继续这样的推理, X 的包含 u 的连通分支也含于 B. 因 X 是连通的, $B = V(X)$, 矛盾. □

块图和原图的关系一般来说是很复杂的, 我们只作些初步的讨论.

设 X 是连通 G-对称图, 并设 $\mathcal{B} = \{B_1, B_2, \cdots, B_n\}$ 是 G 在 $V = V(X)$ 上的一个非平凡完全块系. X 关于 $\mathcal{B}$ 的块图是 $\overline{X}$. 设 B, C 是 $\overline{X}$ 中两个相邻的块, 取 $v \in B$ 满足 $X_1(v) \cap C \neq \varnothing$. 设 $y := |X_1(v) \cap C|$, $x := \|[B \cup C]\|$, 即图 $[B \cup C]$ 的边数, 而图 $[B \cup C]$ 是由 $B \cup C$ 在 X 中的诱导子图. 则由 X 和 $\overline{X}$ 的 G-对称性, x 和 y 与块 B,C 和点 v 的选择无关. 这时我们有下面的

引理 5.3 *在以上的假定下, 再设块长为 $|B| = b$, X 的度数为 k, $\overline{X}$ 的度数为 $\bar{k}$. 则*

(1) $X_1(v) \cap C$ 是 G_v 在 $X_1(v)$ 上的块，于是 $y \mid k$.

(2) $y \mid x$.

(3) $\bar{k} = kb/x$.

证 (1) 设与点 v 相邻的块为 $C = C_1, C_2, \cdots, C_s$. 于是 G_v 作为 G 的子群也置换诸块 $C_1, \cdots, C_s$, 当然也置换诸子集 $X_1(v) \cap C_1, \cdots, X_1(v) \cap C_s$. 因为这些子集的并为 $X_1(v)$, 而 G_v 在 $X_1(v)$ 上传递，故诸子集 $X_1(v) \cap C_i$ 是 G_v 的块. 由此得 $y \mid k$.

(2) 设在块 B 中有 t 个点 $v_i, i = 1, \cdots, t$ 使得 $X_1(v_i) \cap C \neq \varnothing$, 则 $|X_1(v_i) \cap C| = y$. 于是 $x = yt$, 故 $y \mid x$.

(3) 由简单计算可得. □

由这个引理可以看出，块图的度数可以大于、等于或小于原图的度数. 而对于两个相邻的块，并非由一个块的任意一点都有边连到另一块的某一点. 如果考虑群 G 在完全块系上作用的核 K, 那么 K 在某一块 B 上的作用可以是传递的，也可以是不传递的，还可以是平凡的，即 $K = 1$. 由此可见块图和原图之间关系的复杂性. 因此，为决定非本原对称图，先决定它的块图 (块图具有较小的阶), 然后由块图和原图的关系再设法决定原图的路线往往是不能成功的，除非对于非常简单的情形.

为了探寻起码从理论上来说是可行的路线，我们还要引进下面的定义.

定义 5.4 沿用定义 5.1 的符号，称块图 $\overline{X}$ 是 G-正规的，如果 $\mathcal{B}$ 是 G 的某个正规子群 N 的轨道集合. 或者等价的，G 在 $\mathcal{B}$ 上的作用的核 K 在每一块 $B \in \mathcal{B}$ 上的作用是传递的. (这时自然有 $K \geq N$.)

这时我们称原图 X 是块图 $\overline{X}$ 的一个 *伪覆盖*. 又如果在块图 $\overline{X}$ 的任意两个相邻的块之间的诱导子图都是 b 个 K_2 的并，其中 b 是块长，我们称原图 X 是块图 $\overline{X}$ 的一个 *覆盖*.

引进这个定义是基于下面的考虑：决定一个图的所有弧传递的覆盖和伪覆盖比决定以这个图为块图的所有可能的原图要容易

得多. 尽管这在事实上是对的, 但决定前者也绝非易事, 目前还很少有关于图的弧传递覆盖的结果. 但是关于图覆盖的一般研究已经是拓扑图论的一个分支.

定义 5.5 称传递置换群为*拟本原的*, 如果它的每个非平凡正规子群都是传递的.

称 G-对称图 X 为 G-*拟本原的*, 如果 G 在点集 $V(X)$ 上是拟本原群. 称对称图 X 为*拟本原的*, 如果它的自同构群 $\mathrm{Aut}(X)$ 在点集 $V(X)$ 上是拟本原群.

由上述两个定义不难看出, 每个对称图都是某个 G-拟本原图的伪覆盖. 因此我们可以把决定对称图的问题化为决定 G-拟本原对称图以及决定它们的伪覆盖这样两个问题.

而对于拟本原群, 我们有类似本原群的 O'Nan-Scott 定理的结果, 可见下述文章:

C.E. Praeger, An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs, *J. London Math. Soc.*, **(2) 47** (1993), 227–239.

因此, 群论的工具, 特别是有限单群分类定理就可以应用到拟本原群以及拟本原对称图的研究中去.

以上所描述的只是决定对称图的一个理论上的框架, 真正的实现往往只能在对称图的某些子类中获得成功.

对称图的一个特别重要的子类是所谓*局部本原对称图*.

定义 5.6 称 G-对称图 X 为 G-*局部本原的*, 如果对 X 的任一顶点 v, 稳定子群 G_v 在 v 的邻域 $X_1(v)$ 上的作用是本原的. 而称对称图 X 为*局部本原的*, 如果它是 $\mathrm{Aut}(X)$-局部本原的.

对于 G-局部本原的 G-对称图, 我们仍设 $\mathcal{B}=\{B_1,B_2,\cdots,B_n\}$ 是 G 在 $V=V(X)$ 上的一个非平凡完全块系, 并设 $n>2$, 这保证 X 关于 $\mathcal{B}$ 的块图 $\overline{X}$ 不是 K_2. 于是在引理 5.3 中有 $y<k$. 再由 X 的局部本原性以及引理 5.3(1), 我们推得 $y=1$. 这时如果我们再假定 $\overline{X}$ 是 G-正规块图, 则由引理 5.3(3), 推知块图的度数 $\bar{k}$ 与原图的度数 k 相等, 并且 X 是 $\overline{X}$ 的覆盖. 我们写成下面的定理.

定理 5.7 设 X 是 G-局部本原的 G-对称图. 则下列之一成立:

(1) G 是 $V(X)$ 上的拟本原群;

(2) X 是二部图;

(3) X 是 $\overline{G}$-拟本原的 $\overline{G}$-局部本原 $\overline{G}$-对称图 $\overline{X}$ 的一个覆盖, 其中 $\overline{G}$ 是 G 的一个真同态像.

证 设 (1) 不发生, 则 G 存在非传递的非平凡正规子群. 设 N 是 G 的极大非传递正规子群. 如果 N 在 $V(X)$ 上有两个轨道, 则这两个轨道就构成了二部图的二部划分, 于是 X 是二部图, (2) 发生. 这时只剩下 N 有多于二个轨道的情形. 令 $\mathcal{B}=\{B_1,B_2,\cdots,B_n\}$ 是 N 在 $V(X)$ 上的轨道的集合, $\overline{X}$ 是 X 关于 $\mathcal{B}$ 的块图. 再令 $\overline{G}=G/N$, 则由 N 的极大性, $\overline{G}$ 在 $V(\overline{X})$ 上作用忠实. 由本定理前面的那段话已经说明了 X 是 $\overline{X}$ 的覆盖. 为完成证明, 只须证 $\overline{X}$ 是 $\overline{G}$-局部本原的.

为此首先我们证明 N 在 $V(X)$ 上是半正则的, 即对任意的 $v\in V(X)$ 有 $N_v=N\cap G_v=1$. 因为 N_v 不动 $X_1(v)$, 也不动所有的块, 若设 v 含于块 B, 块 C 与块 B 相邻, 即 $C\in\overline{X}_1(B)$, 则 N_v 不动 $X_1(v)\cap C$. 由 G 的局部本原性以及块数大于 2, 有 $|X_1(v)\cap C|=1$, 即 N_v 不动 $X_1(v)$ 中属于块 C 的那个顶点. 由 C 的任意性, N_v 不动 $X_1(v)$ 中的每个顶点. 再由 X 的连通性, 得 $N_v=1$.

下面我们证明 $G_v^{X_1(v)}$ 与 $\overline{G}_B^{\overline{X}_1(B)}$ 置换同构, 于是 $\overline{G}_B$ 也是本原群, 即 $\overline{X}$ 是 $\overline{G}$-局部本原的. 首先我们建立 $\overline{X}_1(B)$ 到 $X_1(v)$ 的一个一一对应, 由前面的叙述这可由 $C\in\overline{X}_1(B)$ 对应到 $C\cap X_1(v)$ 来实现. (验证这确是单射也是满射.) 又容易验证 $\overline{G}_B=G_{\{B\}}/N=G_vN/N$. 这时由 $N\cap G_v=1$ 有映射 $g\mapsto gN$, $g\in G_v$, 是 $G_v^{X_1(v)}$ 到 $\overline{G}_B^{\overline{X}_1(B)}$ 上的同构, 并且是置换同构. 证毕. □

由上述定理可以看出, 决定拟本原的局部本原对称图是很基本的步骤. 但目前在这方面的工作还较少, 值得提出的有以基柱为某些单群 (如 Suzuki 单群和 Ree 型单群) 的几乎单拟本原群为自同构群的 2-弧传递图的分类等. 感兴趣的读者可参看下列文章:

(1) 方新贵和 C.E. Praeger, Finite two-arc transitive graphs admitting a Suzuki simple group, *J. Combin. Theory Ser. B*, 即将刊出.

(2) 方新贵和 C.E. Praeger, Finite two-arc transitive graphs admitting a Ree simple group, *J. Combin. Theory Ser. B*, 即将刊出.

关于局部本原对称图的一个子类是素数度的对称图. 下面的属于 Lorimer 的定理 5.10 给出这类图的自同构群的一个描述. 为了证明 Lorimer 定理, 我们需要下面的概念和引理.

定义 5.8 设 X 为无向连通图, $G \leq \mathrm{Aut}(X)$. 称 X 为 *G-局部传递的*, 如果对于任一点 $v \in V(X)$, G 对于点 v 的稳定子群 G_v 在点 v 的邻域 $X_1(v)$ 上是传递的. 称 X 为 *局部传递的*, 如果 X 是 $\mathrm{Aut}(X)$-局部传递的.

引理 5.9 *G-局部传递无向连通图 X 或为 G-点传递的, 或为二部图.*

证 由定义可看出, 任二距离为 2 的两点属于同一个 G-轨道. (因为首先它们属于同一个 G_v-轨道, 其中 v 是任一与此二点相邻的点.) 于是任二距离为偶数的点属于同一个 G-轨道. 这样 G 在 $V(X)$ 上至多有两个轨道. 如果 X 不是 G-点传递的, 则 G 在 $V(X)$ 上恰有两个轨道, 并且属于同一轨道的二点间不能有边相连, 于是 X 是二部图. □

定理 5.10 *设 X 是连通对称图, 其度数为素数 p. 设 $G \leq \mathrm{Aut}(X)$, 且 G 在 X 上作用弧传递, 但 G 的每个真子群在 X 上作用均非弧传递. 则下列之一成立:*

(1) G 是非交换单群;

(2) G 有正则正规子群 N 且 $G = N \rtimes Z_p$;

(3) X 是二部图;

(4) G 有非平凡的正规子群 N, 且 $\overline{G} = G/N$ 是非交换单群. N 在 $V(X)$ 上有多于二个轨道, X 是其对应的块图的 $\overline{X}$ 的一个覆盖, $\overline{X}$ 的度数亦为 p, 且为 $\overline{G}$-对称的.

证　假定 X 不是二部图，我们要证明 (1), (2) 或 (4) 有一发生.

首先我们注意到，G 的每个真正规子群 N 必为半正则的. 这因为对任一点 $v \in V(X)$, 有 $N_v^{X_1(v)} \trianglelefteq G_v^{X_1(v)}$. 于是 N_v 在 $X_1(v)$ 上或传递或平凡. 若前者发生，则由 G 的点传递性，X 是 N-局部传递的. 又因 X 不是二部图，由引理 5.9, N 必点传递，于是 N 在 X 上作用也弧传递，与 G 的极小性相矛盾. 因此必有 $N_v^{X_1(v)} = 1$, $\forall v \in V(X)$. 再由 X 的连通性, 得 $N_v = 1$, $\forall v \in V(X)$, 即 N 是半正则的.

现在设 N 是 G 的极大真正规子群. 我们区分下列情况：

(a) $N = 1$, 这时 G 是单群. 又因 G 的点稳定子群 G_v 非平凡，G 显然是合数阶的，于是 G 是非交换单群，(1) 发生.

(b) N 在 $V(X)$ 上正则，即 N 在 $V(X)$ 上只有一个轨道. 这时 X 是 N 的 Cayley 图，我们可把 N 和 $V(X)$ 等同看待，并设 $X = \mathrm{Cay}(N, S)$. 由 N 的传递性，有 $G = N \rtimes G_1$, 其中 1 是群 N 的单位元素. 因 G_1 正规化 N, 由定理 4.22(1), $G_1 \leq \mathrm{Aut}(N)$. 因 X 连通，S 生成 N. 于是 N 的每个非平凡自同构在 N 上作用非平凡. 由 X 是 G-对称的，G_1 在 S 上传递，于是 $p \mid |G_1|$. 取 G_1 中的任一 p 阶元 α, 令 $H = \langle \alpha \rangle$. 则 H 在 S 上作用传递，于是 $N \rtimes H$ 在 X 上作用对称. 由 G 的极小性有 $G = N \rtimes H$, 于是 $G_1 = H \cong Z_p$. (2) 成立.

(c) N 在 $V(X)$ 上有两个轨道. 这时 X 是二部图，与假设矛盾.

(d) N 在 $V(X)$ 上有多于两个轨道. 由 N 的极大性，$\overline{G} = G/N$ 是非交换单群，并因此是拟本原的. 于是由定理 5.7, (4) 发生. □

这个定理和它的一个推广的原始文献可见下列二文：

P. Lorimer, Vertex transitive graphs: symmetric graphs of prime valency, *J. Graph Theory* **8** (1984), 55-68.

C.E. Praeger, On minimal symmetric automorphism groups of finite symmetric graphs, *Australasian J. Combinatorics* **4** (1991),

237-252.

作为上述定理的一个应用， Lorimer 在下列文章中决定了所有不是二部图也不是群的 Cayley 图的点数至多为 120 的三度对称图：

P. Lorimer, Trivalent symmetric graphs of order at most 120, *European J. Combin.* **5** (1984), 163-171.

关于对称图的分类，还值得提出的是近年来完成了阶为二不同素数乘积的对称图的完全分类，它在本质上来说也是沿着本节描述的方法来实现的．可参看下列文章：

Ru-Ji Wang and Ming-Yao Xu, A classification of symmetric graphs of order $3p$, *J. Combin. Theory Ser. B*, **58** (1993), 197–216.

C.E. Praeger, Ru-Ji Wang and Ming-Yao Xu, Symmetric graphs of order a product of two distinct primes, *J. Combin. Theory Ser. B*, **58** (1993), 299–318.

为了说明如何用群论方法来决定具有某些条件的对称图，我们给出一个例子．

例 5.11 决定所有互不同构的 10 阶对称图．

解 容易看出，连通的 2 阶和 5 阶对称图只有 K_2, C_5 和 K_5. 于是，不连通的 10 阶对称图只有 $10K_1$, $5K_2$, $2K_5$ 和 $2C_5$.

下面再考虑连通的情况．设 $X \neq K_{10}$ 是一个连通的 10 阶对称图， $A = \mathrm{Aut}(X)$. 区分 A 本原和非本原两种情况．

首先设 A 本原．由第 XII 章例 4.15 和 4.17 知 10 阶点本原图只有 Petersen 图及其补．它们的自同构群同构于 S_5 在 $\Omega = \{1,2,3,4,5\}$ 的 10 个二元子集上的作用．

再设 A 非本原．设 B 是 A 的一个极小的非本原集．记 $|B| = b$, 于是 $b = 2$ 或 5. 再设 $\mathcal{B} = \{B = B_0, B_1, \cdots, B_n\}$, $n = 10/b$, 是包含 B 的完全非本原系．设 X 关于 $\mathcal{B}$ 的商图为 $\overline{X}$, A 诱导出商图的一个自同构群 $\overline{A} = A/K$, 其中 K 是 A 在 $\mathcal{B}$ 上作用的核．分两种情况： (1) K 在 B 上作用非忠实； (2) K 在 B 上作用忠实．

(1) K 在 B 上作用非忠实：设 B_i 和 B_j 是任意两个相邻的块．则 $K_{(B_i)}^{B_j} \neq 1$．因为 $K_{(B_i)}^{B_j} \trianglelefteq K^{B_j}$，有 $K_{(B_i)}^{B_j}$ 传递．于是 X 必为字典式积，这时得到 $K_{5,5}$, $C_5[2K_1]$ 和 $K_5[2K_1]$ 三个图．

(2) K 在 B 上作用忠实：这时区分 $b=5$ 和 2 两种情形．

(i) $b=5$：这时只有两块 B_0 和 B_1，$A_{\{B_0\}}$ 也不动 B_1，即 $K=A_{\{B_0\}}$ 在每块上传递．先设 K 在 B_0 上 2 重传递，任取 $v \in B_0$，则存在 $u \in B_1$ 使 K 不动 u，但在 $B_1 \setminus \{u\}$ 上传递．这样 v 若与 $B_1 \setminus \{u\}$ 中一点连接，则必与其中每一点连接．这推出 X 为 $K_{5,5}$, $5K_2$ 和 $K_{5,5}-5K_2$ 中的一个．但前两个图已在前面出现，故这里只得到 $K_{5,5}-5K_2$ 一个新图．再设 K 在 B_0 上不 2 重传递，这时 K 为 Frobenius 群 $Z_5 \rtimes Z_4$ 的真子群．于是由 X 的度数 ≥ 2 及连通性，得 $K \cong Z_5 \rtimes Z_2$．且 X 的度数为 2．这时 $X=C_{10}$．

(ii) $b=2$：并可假定这时没有长为 5 的块．我们要证明这时没有新的图出现．因 K 在诸块上作用忠实，得 $K=1$ 或 $K=Z_2$，于是 $K \leq Z(A)$．如果 $\overline{A}$ 可解，则 $\overline{A}$，继而 A 有 5 阶正规子群，推出 A 有长为 5 的块，与假设矛盾．这样 $\overline{A}$ 包含一个子群 $\overline{G} \cong A_5$．我们断言 $\overline{G}$ 的原像 G 也在 $V(X)$ 上传递：若否，则 G 必为 A 的指数为 2 的正规子群，它的轨道为长为 5 的块，矛盾．如果 $K=1$，$G \cong A_5$，这时有点稳定子群 G_v 的阶为 6．但因 6 阶子群在 A_5 中是极大子群，G 为本原群，与假设矛盾．故必有 $K=Z_2$，这时 G 是 Z_2 被 A_5 的中心扩张．又因 G 有长为 2 的块，它可看作 $Z_2 \wr A_5$ 的子群，于是必有 $G=H \times K$，其中 $H \cong A_5$．这时点稳定子群 G_v 的阶为 12．如果 $G_v \leq H$，则 H 对应于长为 5 的块，矛盾．故 $G_v \cap H$ 为 H 的 6 阶子群，为 H 的极大子群，并从而 G_v 为 G 之极大子群，又得到 G 为本原群，矛盾于我们的假设． □

在结束本节时，我们证明一个关于无向连通对称图的点稳定子群的结果，它可以看作是第 XII 章定理 4.12 的推广．

定理 5.12 *设 X 是无向连通 G-对称图，$v \in V(X)$．设 K 是点稳定子群 G_v 的一个合成因子．则 K 同构于 $G_v^{X_1(v)}$ 的一个截断．*

证 设 $H \le G_v$ 满足条件: (1) H 有合成因子 K, (2) H 的每个真子群都没有合成因子同构于 K. 如果 H 在 $X_1(v)$ 上作用非平凡, 则 K 显然是 $G_v^{X_1(v)}$ 的合成因子, 定理得证. 如果 H 在 $X_1(v)$ 上作用平凡, 则 $H \le G_u$, 其中 $u \in X_1(v)$. 这时考虑 H 在 u 的邻域 $X_1(u)$ 上的作用, 如果 H 在 $X_1(u)$ 上作用非平凡, 则 K 是 $G_u^{X_1(u)}$ 的合成因子, 而 $G_u^{X_1(u)} \cong G_v^{X_1(v)}$, 定理亦得证. 因此可设对任一 $u \in V(X)$, 只要 $H \le G_u$, 都有 H 在 $X_1(u)$ 上作用平凡. 但由 X 的连通性, 这将推出对每一 $u \in V(X)$, 都有 $H \le G_u$. 而这又推出 $H = 1$, 矛盾. 定理证毕. □

这个定理的另一证明可见下文:

P.M. Neumann, Finite permutation groups, edge-coloured graphs and matrices, in *Topics in Group Theory and Computation*, (Proc. of a summer school at University College, Galway, 1973); Edited by M. P. J. Curran, Academic Press, 1977. Chap. 5, pp. 82–118.

习 题

3. 试决定所有的 6 阶无向对称图.

4. 试决定所有的 8 阶无向对称图.

5. 试决定所有的 13 阶无向对称图.

6. 设 $G = \{0, 1, \cdots, p-1\}$ 是写成加法形式 (mod p) 的素数 p 阶循环群, 即域 $GF(p)$ 的加法群, $p \ge 3$. 则 $\mathrm{Aut}(G) \cong Z_{p-1} = \{1, 2, \cdots, p-1\}$, 后者看成是域 $GF(p)$ 的乘法群. 设 H 是 $\mathrm{Aut}(G)$ 的一个偶阶子群. 令 $X = \mathrm{Cay}(G, H)$, 这里 H 看成是 G 的子集. 证明 X 是 p 阶对称图.

7. 证明每个 p 阶对称图都可由第 6 题的方法构造出来.

§6. 半传递图和半对称图

本节所讲述的半传递图和半对称图是两类有趣的图类, 尽管它们的研究并不是群与图这个分支的主流. 我们讲述它们的目的是想通过它们的研究来看群论方法是怎样应用到对称性比较强的图的理论中去的.

先看所谓的 *半传递图*. 我们有下面的

定义 6.1 设 X 是无向简单图，$G \le \mathrm{Aut}(X)$. 称 X 为 G-半传递的，如果 G 在图 X 上的作用是点传递且边传递的，但不是弧传递的. 称 X 为半传递图，如果 X 是 $\mathrm{Aut}(X)$-半传递的. 半传递图也叫做 $\frac{1}{2}$-传递图.

Tutte 证明了下列定理.

定理 6.2 *设 X 是无向简单图，$A = \mathrm{Aut}(X)$. 又设 X 是点传递且边传递的，并为奇数 k 度正则的，则 X 必为弧传递的. 这说明不存在奇数度的半传递图.*

证 取定 X 的一条边 $\{u,v\}$, 则 (u,v) 和 (v,u) 是和它对应的两条弧. 令 $\Omega_1 = (u,v)^A = \{(u,v)^g \mid g \in A\}$, $\Omega_2 = (v,u)^A = \{(v,u)^g \mid g \in A\}$. 由 X 的边传递性，$\Omega_1 \cup \Omega_2 = A(X)$, 这里 $A(X)$ 是 X 的弧集. 如果 X 不是弧传递的，则 $\Omega_1 \cap \Omega_1 = \varnothing$, 即对于任一弧 (x,y), 都不存在 $g \in A$ 使得 $(x,y)^g = (y,x)$. 现在取定一个点 v 和弧的一个轨道 Ω_1, 令 $X_v = \{x \mid (v,x) \in \Omega_1\}$, $Y_v = \{y \mid (y,v) \in \Omega_1\}$. 则 $X_v \cap Y_v = \varnothing$, 于是 v 的邻域 $X_1(v) = X_v \cup Y_v$, 由此推出 X 的正则度数 $k = |X_v| + |Y_v|$. 又由 X 的点传递性，对于任意的顶点 $u \in V(X)$, 有 $|X_v| = |X_u|$, $|Y_v| = |Y_u|$. 于是 X 的边数等于 $|X_v||V(X)|$, 又等于 $|Y_v||V(X)|$, 这推出 $|X_v| = |Y_v|$, 即 k 是偶数，矛盾. □

这个定理说明半传递图必有偶数度数，而 Bouwer 证明对于任一偶数 $k > 2$, 都至少存在一个 k 度半传递图. （2 度正则图是若干个圈的并，当然由点传递性和边传递性可推出弧传递性. 即不存在 2 度半传递图.）有兴趣的读者可参看下文：

I. Z. Bouwer, Vertex and edge-transitive but not 1-transitive graphs, *Canad. Math. Bull.* **13** (1970), 231–237.

最小的半传递图是一个有 27 个顶点的 4 度正则图，它是 Holt 在 1981 年给出的. 后来人们对它又有很多研究. 首先人们发现这个由 Holt 用组合方法定义的图是 27 阶亚循环群的 Cayley 图，进而证明它具有最小可能的点数，后来又证明具有 27 个顶点的 4 度半传递图是唯一的. 有兴趣的读者可参看下列文章：

(1) D.F. Holt, A graph which is edge transitive but not arc-transitive, *J. Graph Theory*, **5** (1981), 201–204.

(2) B. Alspach, D. Marušič and L. Nowitz, Constructing graphs which are 1/2-transitive, *J. Austral. Math. Soc.*, **56** (1994), 391–402.

(3) Ming-Yao Xu, Half-transitive graphs of prime-cube order, *Journal of Algebraic Combinatorics*, **1** (1992), 275–282.

下面我们将在例 6.5 中给出 Holt 图的定义，并证明它是半传递的. 在此之前我们先证明几个引理.

设

$$G = \langle a, b \mid a^9 = b^3 = 1, b^{-1}ab = a^4 \rangle. \tag{6.1}$$

则 G 是 27 阶亚循环群. 我们有

引理 6.3 *G 的自同构群* $\mathrm{Aut}(G)$ *的阶为* $2\cdot 3^3 = 54$, *且* $\mathrm{Aut}(G)$ *由下列元素生成*:

$$\begin{aligned} \alpha &: a \mapsto a, & b &\mapsto ba^3, \\ \beta &: a \mapsto a^4, & b &\mapsto b, \\ \gamma &: a \mapsto ba, & b &\mapsto b, \\ \delta &: a \mapsto a^{-1}, & b &\mapsto b. \end{aligned}$$

证 直接计算得 $\alpha, \beta, \gamma, \delta$ 是群 G 的自同构.

设 τ 是 G 的任一自同构: $a^\tau = b^i a^j$, $b^\tau = b^k a^s$. 因 a^τ 的阶为 9, 而 b^τ 的阶为 3, 我们有 $3 \nmid j$ 并且 $3 | s$. 因 $(b^\tau)^{-1} a^\tau b^\tau = (a^\tau)^4$, 并注意到 $a^3 \in Z(G)$ 以及 G 是 3-交换群 (参看 X, 定义 2.1), 我们有

$$b^{-k}(b^i a^j) b^k = (b^i a^j)^4,$$

$$b^i a^{j4^k} = b^i a^{4j}.$$

于是 $j4^k \equiv 4j \pmod 9$, 这推出 $k \equiv 1 \pmod 3$. 这样我们可以假设 $a^\tau = b^i a^j$, $b^\tau = ba^{3t}$, 其中 i 和 t 至多有 3 种选择, 而 j 至多有 $9-3=6$ 种选择. 这样 $|\mathrm{Aut}(G)| \le 3^3 \cdot 2$. 但已有 $|\langle \alpha, \beta, \gamma, \delta \rangle| = 3^3 \cdot 2$, 于是 $\mathrm{Aut}(G) = \langle \alpha, \beta, \gamma, \delta \rangle$. □

引理 6.4 设 $\{x,y\}$ 是 G 的生成集，令 $S=\{x,y,x^{-1},y^{-1}\}$，$X=\mathrm{Cay}(G,S)$，$A=\mathrm{Aut}(X)$. 设 $R(G)$ 是 G 的右乘变换群. 则 $R(G)$ 是 A 的正规子群，即 X 是 G 的正规 Cayley 图.

证 首先证明下面的事实.

(1) 设 $\mathrm{Aut}(G,S)=\{\alpha\in\mathrm{Aut}(G)\mid S^{\alpha}=S\}$，则 $|\mathrm{Aut}(G,S)|\le 2$：设 $\alpha\in\mathrm{Aut}(G,S)$. 则 x,y 在 α 下的像只能是 $x^{\pm1},y^{\pm1}$. 对于所有可能的情况，易验证都有 $\alpha^4=1$. 于是 $\mathrm{Aut}(G,S)$ 是 2-群. 又，$\mathrm{Aut}(G,S)$ 必为 $\mathrm{Aut}(G)$ 的子群，由引理 6.3 得 $|\mathrm{Aut}(G,S)|\le 2$.

(2) $|A|=2^m3^3$ 对某个非负整数 m 成立：首先我们有 $A=R(G)A_1$，其中 A_1 是 1 的点稳定子群. 因 X 是 4 度连通图，由定理 5.12，A_1 是 $\{2,3\}$-群. 于是 $|A|=2^m3^n$，其中 m 是非负整数，而 $n\ge 3$. 若 $n>3$，则 $N_A(R(G))$ 的 Sylow 3-子群的阶至少为 3^4. 但据命题 4.22(1) 有 $N_A(R(G))=R(G)\mathrm{Aut}(G,S)$，与事实 (1) 相矛盾.

(3) A_1 是 2-群，$O_2(A)=1$ 并且 $C_A(O_3(A))\le O_3(A)$：由 (2)，显然 A_1 是 2-群，并且是 A 的 Sylow 2-子群. 因为 A_1 作为传递置换群的点稳定子群是无核的，即 $\mathrm{Core}_A(A_1)=1$，于是 $O_2(A)=1$. 最后由 A 是 $\{2,3\}$-群，因而是可解的，由上册第 V 章习题 6 有 $C_A(O_3(A))\le O_3(A)$.

下面我们用反证法证明引理的结论. 假定结论不真，即 $O_3(A)<R(G)$. 则有

(4) $O_3(A)\cong Z_3\times Z_3$：只须证 $O_3(A)$ 非循环. 若 $O_3(A)$ 循环，设其阶为 3^k，则 $|\mathrm{Aut}(O_3(A))|=2\cdot 3^{k-1}$. 又由 N/C 定理，$A/C_A(O_3(A))=A/O_3(A)\lesssim\mathrm{Aut}(O_3(A))$. 于是 $|A|$ 的 2-因子最大为 2，这推出 $R(G)\trianglelefteq A$，与假设矛盾.

(5) 最终矛盾的推出：因为 $O_3(A)\cong Z_3\times Z_3$，我们有 $A/O_3(A)=A/C_A(O_3(A))\lesssim\mathrm{Aut}(O_3(A))\cong GL(2,3)$，因而 $A\lesssim AGL(2,3)$. 容易看出仿射群 $AGL(2,3)$ 的 Sylow 3-子群是方次数为 3 的 27 阶群，而 A 的 Sylow 3-子群为方次数为 9 的亚循环群，矛盾. □

下面的例子就是著名的 Holt 图，但是我们的定义与 Holt 最初的定义很不一样.

例 6.5 设 G 是 (6.1) 式定义的 27 阶亚循环群. 设 $S = \{x, y, x^{-1}, y^{-1}\}$, $x = ba$, $y = ba^{-1}$. 设 $X = \mathrm{Cay}(G, S)$. 则 X 是 27 阶 4 度半传递图.

证 我们需要证明 X 是边传递的，但不是弧传递的.

设 $A = \mathrm{Aut}(X)$. 因 X 是点传递的，为证 X 边传递，只须证明与 1 关联的 4 条边属于 A 在边集合上的同一轨道. 注意到 $\delta : a \mapsto a^{-1}$, $b \mapsto b$ 是群 G 的自同构，因而也是图 X 的自同构，我们有 $\{1, x\}^{\delta} = \{1, (ba)^{\delta}\} = \{1, ba^{-1}\} = \{1, y\}$. 又，右乘变换 $R(x^{-1})$ 把边 $\{1, x\}$ 变到边 $\{1, x^{-1}\}$, 而右乘变换 $R(y^{-1})$ 把边 $\{1, y\}$ 变到边 $\{1, y^{-1}\}$, 故得 X 的边传递性.

最后证明 X 不是弧传递的. 由于 X 是 G 的正规 Cayley 图 (引理 6.4), 我们有 $\mathrm{Aut}(X) = R(G)\mathrm{Aut}(G, S)$, 于是 $|\mathrm{Aut}(X)| = |G||\mathrm{Aut}(G, S)| \le 2|G|$ (引理 6.4 的证明中的事实 (1)). 但若 X 为弧传递，则 $|\mathrm{Aut}(X)| \ge 4|G|$, 矛盾. □

事实上， Holt 图是 (在同构意义下) 唯一的 27 阶 4 度半传递图，它的证明留给读者作为习题.

近年来，关于半传递图的研究很为活跃，可参看下列文章：

徐明曜， Some new results on 1/2-transitive graphs, 数学进展, **23** (1994), 505–516.

下面转而介绍所谓 半对称图. 首先我们给出它的定义.

定义 6.6 称无向简单图为 半对称图, 如果它是边传递的正则图，但不是点传递的.

命题 6.7 设 X 为半对称图， $A = \mathrm{Aut}(X)$. 则 A 在 $V(X)$ 上恰有两个轨道，譬如说是 $U(X)$ 和 $W(X)$. 这时 X 是二部图， $V(X) = U(X) \cup W(X)$ 构成了 X 的二部划分，并且有 $|U(X)| = |W(X)|$.

证 首先，半对称图不会是空图，即 $E(X)$ 非空. 任取一条边 $\{u, w\} \in E(X)$. 令 $U(X) = \{u^g \mid g \in G\}$, $W(X) = \{w^g \mid g \in G\}$.

则由边传递性，得 $V(X)=U(X)\cup W(X)$. 又由 X 非点传递，$U(X)\cap W(X)=\varnothing$. 最后，由 X 的正则性，必然推得 $|U(X)|=|W(X)|$. □

§4.4 讲过 Sabidussi 陪集图. 在那里我们证明了每个点传递图都是适当构造的 Sabidussi 陪集图. 与其类似，半对称图也有相似的构造方法. 这种构造方法还适应于更广泛的一个图类，即所谓半点传递图. 我们给出下列定义.

定义 6.8 称具有二部划分 $V(X)=U(X)\cup W(X)$ 的二部图 X 为*半点传递图*, 如果 X 的自同构群 $\mathrm{Aut}(X)$ 在 $U(X)$ 和 $W(X)$ 上都是传递的.

注意，半点传递图不一定边传递，其二部划分中的 $U(X)$ 和 $W(X)$ 也不一定等势. 但另一方面，半点传递图也可能是点传递的.

下面我们给出群的*双陪集图*的定义.

定义 6.9 设 G 是有限群，L 和 R 是 G 的两个子群. 设 D 是若干个形如 RgL 的双陪集的并. 我们定义 G 关于 L,R 和 D 的*双陪集图* $X=\mathbf{B}(G,L,R;D)$ 如下：

$$\begin{aligned} V(X) &= [G:L]\cup[G:R], \\ E(X) &= \{\{Lg,Rdg\}\mid g\in G,d\in D\}. \end{aligned}$$

与 Sabidussi 陪集图相同，因为我们不考虑重图，如果 $Rdg=Rd_1g$, 我们认为边 $\{Lg,Rdg\}$ 和 $\{Lg,Rd_1g\}$ 是同一条边.

由此定义我们不难看出双陪集图是 Sabidussi 陪集图的推广.

下面的两个命题是基本的，也是容易证明的，但我们略去它的证明.

命题 6.10 *设 $X=\mathbf{B}(G,L,R;D)$ 是 G 关于 L,R 和 D 的双陪集图. 则*

(1) *X 是良定义的二部图.*

(2) 形如 Lg 的顶点的度数是 $|D:R|$, 形如 Rg 的顶点的度数是 $|D:L|$. 因此, X 是正则图当且仅当 $|L|=|R|$.

(3) $\mathrm{Aut}(X)$ 包含 G (依右乘变换作用在 $[G:L]$ 和 $[G:R]$ 上), 于是 X 是半点传递图.

(4) X 是连通的当且仅当 $G=\langle D^{-1}D\rangle$.

(5) X 是 G-边传递的当且仅当 $D=RgL$ 是一个单个的双陪集.

命题 6.11 设 X 是有二部划分 $V(X)=U(X)\cup W(X)$ 的半点传递图, $A=\mathrm{Aut}(X)$. 取 $u\in U(X)$, $w\in W(X)$. 令 $L=A_u$, $R=A_w$, $D=\{g\in G \mid w^g\in X_1(u)\}$. 则 D 是形如 RgL 的双陪集的并, 且满足 $X\cong \mathbf{B}(G,L,R;D)$.

由以上两个命题, 为了决定半对称图, 只须从满足条件 $|R|=|L|$ 以及 $D=RgL$ 是一个单个的双陪集的双陪集图 $\mathbf{B}(G,L,R;D)$ 中选择非点传递的那些. 下面我们在例 6.14 中给出一个半对称图的例子, 它的自同构群在其二部划分的两个部分上的作用都是本原的. 这种半对称图叫做*双本原的半对称图*.

为了证明下面的例 6.14 中定义的图确为半对称图, 我们需要 Tutte 关于度 s-弧传递图的一个著名定理. 它的证明可参看本章开头提到的 Biggs 的 "Algebraic Graph Theory".

定理 6.12 (Tutte) 设 X 是 3 度 s-弧传递图. 则 $s\le 5$.

推论 6.13 设 X 是 3 度弧传递图, $A=\mathrm{Aut}(X)$. 则对任一顶点 $v\in V(X)$, v 在 A 中的点稳定子群 A_v 的阶整除 48.

例 6.14 令 $G=PGL(2,11)$, $L\cong S_4$ 和 $R\cong D_{24}$ 是 G 的两个子群, 且满足 $L\cap R\cong D_8$. 令 $D=RL$, $X=\mathbf{B}(G,L,R;D)$. 则 X 是双本原的半对称图.

证 容易验证 G 中确实存在满足上述条件的子群 L 和 R, (验证留给读者.) 注意到 L 和 R 都是 G 的极大子群, 以及 $|D:$

$L| = |D : R| = 3$. 于是 X 是边传递的 3 度正则图，并且 G 在 $[G : L]$ 和 $[G : R]$ 上的作用都是本原的. 因此，只须证 X 不点传递即可完成证明.

假定 X 点传递. 则由定理 6.2, X 必弧传递. 令 $A = \mathrm{Aut}(X)$. 由推论 6.13, 对于任一顶点 v, $|A_v| \mid 48$. 于是只可能发生 $|A_v| = 24$ 和 $|A_v| = 48$ 两种情况. 注意到传递置换群的点稳定子群之间是彼此共轭的，因而也是同构的，第一种情况显然不能发生，（因为 $L \cong S_4$ 和 $R \cong D_{24}$ 不同构.）第二种情况也不能发生，这是因为不可能存在一个 48 阶群，它既存在一个 24 阶子群同构于 S_4, 又存在一个 24 阶子群同构于 D_{24}. 这点请读者自行证明. □

习 题

1. 证明交换群的 Cayley 图不可能是半传递图.

2. 在定义 6.9 中，取 $L = R = 1$, 得到的双陪集图叫做群 G 的双 Cayley 图. 证明交换群的双 Cayley 图不可能是半对称图.

下册习题提示

第 VII 章

4. 由 H 在 $G-\{1\}$ 上传递, $G-\{1\}$ 中元素的阶皆相同, 故必为素数. 进一步证明 G 必初等交换.

5. 考虑半直积 $S=G\rtimes H$, 取 S 的一个主群列以 G 为其中一项.

6. 若 $p \mid |G|$, 则由定理 1.19 及作用的不可约性得 G 是 p-群, 再用命题 1.8. 而若 $p \nmid |G|$, 用定理 3.3.

7. (1) 利用第 1 题得 H 在 $N_G(C)/C_G(C)$ 上作用是平凡的. 再用定理 3.10 可得.

9. 任取 $\alpha\in\Omega$. 令 $K=S_\alpha$, 则 $S=S_\alpha G$. 于是 $H\cong S/G\cong S_\alpha/S_\alpha\cap G$. 由 $(|H|,|G|)=1$ 得 $(|H|,|G\cap S_\alpha|)=1$. 用 Schur-Zassenhaus 定理得 $G\cap S_\alpha$ 在 S_α 中有补 $H_1\cong H$, 于是存在 $g\in G$ 使 $H_1^g=H$. 验证 $\alpha^g=\beta$ 即为 H 之不动点.

不动点的共轭性也用 Schur-Zassenhaus 定理.

10. 考虑半直积 $G\rtimes G$ 通过共轭变换作用在 $\mathrm{Syl}_p(G)$ 上.

12. 用定理 3.6. 例子可考虑 $D_8=G\rtimes H$.

13. 用定理 2.7 和定理 3.10.

14. 令 $S=G\rtimes H$, 则 $H,H^{x^{-1}}\le C_S(K)$, 且易知它们为 $C_G(K)$ 在 $C_S(K)$ 中的补. 由 Schur-Zassenhaus 定理知存在 $a\in C_G(K)$ 使得 $H^{x^{-1}}=H^a$, 令 $y=ax$ 即可.

15. 设 G 为极小阶反例, 则有素数 $p \mid |G|$ 使 $O^p(G)$ 是 G 的极小正规子群, 且 $G/O_p(G)$ 是素数幂阶循环群, 并被 H 中心化.

16. 利用定理 3.10 把问题化成 $[A,K]=1$ 和 $[A,K]=K$ 两种情形, 对第一种情形用定理 3.13 和第 V 章第 5 题; 而对第二种情形则有 $O_{p'}(G)=1$ 并且

$$[K,A\cap O_p(G)]=1=[K,O_p(G)/O_p(G)\cap A].$$

再利用定理 3.6 和第 V 章习题 6.

17. 考虑上中心群列 $1 = Z_0(G) < Z_1(G) < \cdots < Z_c(G) = G$, 用归纳法证明

$$Z_c(G)/Z_k(G) = \prod_{x\in H-\{1\}} C_{Z_c(G)/Z_k(G)}(x).$$

18. 利用推论 3.15.

19. 容易证明 $|\Phi(P)| = 4$, 即 P 为特殊 2-群.

第 VIII 章

3. 采用 Brandis 的证法: 设 K 是使定理不真的极小阶反例. 令 Z 是 K 的中心, 并设 $|Z| = q$, 则 $|K| = q^n$. 再证明:

(1) K 的乘法群 G 不包含 (p,p) 型子群和四元数子群.

(2) G 的 Sylow 子群皆循环.

(3) 若 $G' = \langle a\rangle$, $G = \langle a\rangle\langle b\rangle$, $\langle a\rangle \cap \langle b\rangle$, 则对某个正整数 s, 有 $Z(G) = \langle b^s\rangle$ 是 Z 的乘法群.

(4) 存在正整数 m 和 t 使 $o(a) = \frac{q^m-1}{q-1}$, $o(b) = q^t - 1$. 并由此推出 $n = 1$, 于是 $Z = K$.

4. 用 Grün 第二定理, 不妨设 $P \trianglelefteq G$. 令 H 为 P 在 G 中的补. 考虑 H^a, 其中 $a \in P$, $o(a) = \exp P = p^n$. 令 $P_1 = \Omega_{n-1}(P)$. 因 $|G : P_1H| = p$, 有 $P_1H \trianglelefteq G$, 从而 H^a 与 H 在 P_1H 中共轭, 于是存在 $b \in P_1$ 使 $H^{ab} = H$. 由 $o(ab) = o(a)$, 不妨用 a 替换 ab, 可设 $H^a = H$, 从而 $[a, H] \le H \cap P = 1$. 设 $P = \langle a\rangle \times K$. 用类似的方法知存在 $a_1 \in K$, $o(a_1) = \exp K$, 并且 $[a_1, H] = 1$. 最终可证明 $[P, H] = 1$, $H \trianglelefteq G$, 因此 G 为 p-幂零.

5. 分析极小反例, 应用定理 3.4.

6. 例如 $Q_8 \rtimes Z_3$.

7. 应用第 5 题于 G'.

8. 用定理 3.5(2). 设 $1 \ne U$ 为 G 的任意 p-子群, 则 $H := N_G(U)/C_G(U) \lesssim \mathrm{Aut}(U)$. 对 H 中 p'-元 α, 考虑 α 在 $U/\Phi(U)$ 上作用. 由

$$|\mathrm{Aut}(U/\Phi(U))| \;\Big|\; (p^d-1)(p^{d-1}-1)\cdots(p-1),$$

知 α 在 $U/\Phi(U)$ 上作用平凡, 进而 α 在 U 上作用平凡, $\alpha = 1$.

10. 设 P 是最小阶反例. 并设 $\alpha \ne 1$ 是 P 的最小阶 p'-自同构使得 α 在 P 的每个 α-不变的子群上作用平凡. 考虑半直积 $S = P \rtimes \langle\alpha\rangle$. 证明 S 满足定理 3.4 的条件.

11. 设 $P \in \mathrm{Syl}_p(O_{p'p}(G))$, $N = N_G(P)$. 由 Frattini 论断易知 $\overline{N} = \overline{G}$, 这里 $\overline{G} = G/O_{p'}(G)$. 于是可取 $C \le N$ 使 $\overline{C} = C_{\overline{G}}(O_p(\overline{G}))$. 从而 $[C, P] \le O_{p'}(G) \cap P = 1$, 推出 $C \le C_G(P) \le O_{p'p}(G)$. 这样 $\overline{C} \le O_p(\overline{G})$, 即 $\overline{G}$ 是 p-约束的. 类似地验证 $\overline{G}$ 是 p-稳定的.

12. 唯一性用定理 7.5(2).

13. 只要证 H 中 2 阶元唯一即可.

14. 若 $p=2$, 则 G 交换, 故可设 $p\neq 2$. 用极小反例法, 仿照定理 7.7 的证明. 原证明中步骤 (1) 和 (2) 仍能成立. 为证步骤 (3), 即证 G 非可解, 仍用反证法, 可得 α-不变正规子群 $Q\cong Z_q^m$, 并且有 $G/Q\cong Z_r^n$. 若 $r\neq p$, 则定理证明中方法成立. 若 $r=p$, 进一步讨论可得 $n=1$, 先后应用 VII, 3.8 与 3.15, 即可完成证明. 最后证步骤 (4), 证明存在 α-不变的 Sylow p-子群, 用原方法推出矛盾.

第 IX 章

§1.

1. 令 $\eta: G\to G/N$ 是自然同态, 则 η 映 $C_G(H/K)$ 到 $C_{G/N}((H/N)/(K/N))$ 内. 定义

$$\eta^*(C_G(H/K)x)=C_{G/N}((H/N)/(K/N))\eta(x).$$

证明 η^* 是 $G\big/C_G(H/K)$ 到 $(G/N)\big/C_{G/N}((H/N)/(K/N))$ 的同构.

2. 由命题 1.3, 只需证 $C_G(HK/K)=C_G(H/H\cap K)$. 任意 $x\in C_G(HK/K),[x,hk]\in K$ 对任意 $h\in H,k\in K$ 成立. 由换位子公式, $[x,hk]=[x,k][x,h]^k$, 从而推出 $[x,h]\in H\cap K$ 对任意 $h\in H$ 成立, 即 $x\in C_G(H/H\cap K)$. 类似地证明 $C_G(HK/K)\supseteq C_G(H/H\cap K)$.

3. 先证 G 可解. 设 p 为整除 $|\,G\,|$ 的任一素数, $P\in \mathrm{Syl}_p(G)$. 由假设存在 $B\leq G$ 使得 $G=PB$ 且对任一 $X<B$ 均有 $PX<G$. 令 N 为 B 的任一 Sylow p-子群, 则 PN 为 G 的子群, 故 $N\leq P$. 这说明 B 有唯一的 Sylow p-子群 N, 所以 $N\lhd B$. 由 Schur-Zassenhaus 定理, B 有 p'-Hall 子群, 它也是 G 的 p'-Hall 子群. 由上册第 V 章定理 2.3, G 为可解.

证 G 为超可解. 令 N 为 G 的极小正规子群, $|\,N\,|=p^n$. 由归纳, G/N 超可解. 令 $P\in\mathrm{Syl}_p(G)$. 则 $N\leq P$ 且 $N\cap Z(P)\neq 1$. 取 $x\in N\cap Z(P)$ 为 p 阶元. 利用半正规条件证明 $\langle x\rangle Q=Q\langle x\rangle$ 对 G 的任意 Sylow 子群 Q 成立, 从而 $\langle x\rangle\lhd G$, 故 $|\,N\,|=p, G$ 为超可解.

4. 若 G 超可解, 则 H/K 为 p 阶群, 故得结论. 反之, 设对任一 p 主因子 H/K, $G/C_G(H/K)$ 为循环且方指数整除 $p-1$, 则 H/K 为可解, 故为 p-群, 应用引理 1.9 得 H/K 为 p 阶群.

5. 不失一般性, 设 $\Phi(G)=1$. 要证 G 超可解, 关键是证 $G/C_G(F(G))$ 超可解. 因为 $C_G(F(G))\leq F(G)$. 从而 $G/F(G)$ 超可解, 再由假设立得 G 超可解.

$G/C_G(F(G))$ 超可解可由下述更一般的命题推出. 设 $N \lhd G$ 且 $1 = N_0 < N_1 < \cdots < N_n = N$ 满足 $N_i \lhd G$ 且 $|N_{i+1}/N_i| = p_i$ 为素数, 则 $G/C_G(N)$ 为超可解. 对长度 n 归纳证明.

当 $n=1$ 时, $G/C_G(N_1)$ 是循环群, 结论成立. 当 $n>1$ 时, 由归纳 $G/C_G(N_{n-1})$ 及 $G/C_G(N/N_1)$ 为超可解, 令 $C = C_G(N_{n-1}) \cap C_G(N/N_1)$, 则 G/C 超可解. 再证明 $C/C_G(N)$ 循环, 立得 $G/C_G(N)$ 超可解 (参阅贝. 胡佩特, 有限群论, 第一卷第二分册, 第 368 页, 辅理 9.8).

6 和 7 的证明可参看: 《广西大学学报》, **4**:**2**(1998), 9–13.

§2.

1. 对 $|G|$ 用归纳法.

(1) 若 $O_{p'}(N) > 1$, 则 $l_p(G/N) = l_p(G/O_{p'}(N)\big/N/O_{p'}(N)) \le l_p(G/O_{p'}(N)) = l_p(G)$. 若 $O_{p'}(G) = 1$, 则 $O_p(N) > 1$, 讨论类似.

(2) 不妨设 H 是 G 的一个极大子群. 先令 $O_p(G) > 1$. 若 $O_p(G) \le H$, 则 $l_p(H) \le l_p(H/O_p(G)) + 1 \le l_p(G/O_p(G)) + 1 = l_p(G)$. 若 $O_p(G) \not\subseteq H$, 则 $G = HO_p(G)$. $l_p(H) \le l_p(H/H \cap O_p(G)) + 1 = l_p(G/O_p(G)) + 1 = l_p(G)$. 类似地讨论 $O_{p'}(G) > 1$ 的情形.

(3) 记 $G = N_1N_2$. 只需证 $l_p(G) \le \max\{l_p(N_1), l_p(N_2)\}$. 令 $O_p(G) > 1$, $N_1{}^* = N_1O_p(G)$, $N_2{}^* = N_2O_p(G)$, 则 $l_p(G) = l_p(G/O_p(G)) + 1 \le \max\{l_p(N_1{}^*/O_p(G)), l_p(N_2{}^*/O_p(G))\} + 1$. 而 $l_p(N_1{}^*/O_p(G)) = l_p(N_1/N_1 \cap O_p(G)) = l_p(N_1/O_p(N_1)) = l_p(N_1) - 1$, 同理 $l_p(N_2{}^*/O_p(G)) = l_p(N_2) - 1$, 从而 $l_p(G) \le \max\{l_p(N_1), l_p(N_2)\}$. 类似地讨论 $O_{p'}(G) > 1$ 的情形.

2. $|A_G(H/K)| = |G/C_G(H/K)|$ 并应用定理 1.4 得 $p \nmid |G/F_p(G)|$, 从而推出 $l_p(G) \le 1$.

3. 必要性由定理 2.6(1) 推出. 充分性: 因为 $l_p(G) \le 1$, 所以 $O_{p'p}(G)/O_{p'}(G)$ 同构于 G 的一个 Sylow p-子群, 故得结论.

§3.

1. 对群阶用归纳法. 令 N 为 G 的一个极小正规子群. 则 N 为初等交换 p-群. 存在性: G/N 存在 Carter 子群 H/N. 令集合 $\mathcal{F} = \{M \mid M \le H$ 幂零且满足 $G = MN\}$ 则 $\mathcal{F}$ 是非空的. 证明 $\mathcal{F}$ 的极大元是 G 的 Carter 子群.

共轭性: 令 C_1, C_2 均为 G 的 Carter 子群. 首先证明 C_1N/N 和 C_2N/N 是 G/N 的 Carter 子群. 于是存在 $g \in G$ 使 $C_2N = C_1{}^gN$. 由归纳法可设 $C_2N = G = C_1{}^gN$. 令 H_1, H_2 分别表示 C_1 和 C_2 的 p'-Hall 子群, 则存在 $x \in G$ 能使 $H_2 = H_1{}^x$, 从而 $\langle C_1{}^x, C_2\rangle \le N_G(H_2)$. 若 $N_G(H_2) = G$, 取

$N \leq H_2$, 结论成立. 若 $N_G(H_2) < G$, 由归纳, $C_1{}^x$ 与 C_2 在 $N_G(H_2)$ 中共轭.

2. 令 G 是一个极小阶反例, N 为 G 的一个极小正规子群. G/N 也满足假设, 故为可解. 于是 N 为非可解特征单群. 令 p 为 $|N|$ 的最大素因子, $P \in \mathrm{Syl}_p(N)$. 由引理 1.14, $N_G(P)$ 有合数指数, 故为幂零. 特别地, $N_N(P)$ 为幂零. 由第 VIII 章定理 5.1 推出矛盾.

3. 假设结论不成立. 对 $G/\mathrm{Core}_G(H)$ 应用定理 3.4 和 3.5 导出矛盾.

4. 分两步证明 (a) $G' = [A, B]$, (b) 对任意 $a, a' \in A, b, b' \in B, [a, b]$ 与 $[a', b']$ 可换 (参阅贝. 胡佩特, 有限群论, 第一卷第二分册, 第 313 页, 定理 4.4).

§4.

1. S_4 有 3 个极大子群共轭类, 其代表为 S_3, A_4 及 Sylow 2-子群. 逐一检查即得.

2. 回答否定. 反例 $G = \langle a \rangle \times A_4$, 其中 a 为 2 阶元.

3. 设 G 非超可解. 取 $U \lhd G$ 尽可能大使得 G/U 非超可解. 记 $\overline{G} = G/U$. 则 $\overline{G}$ 有唯一极小正规子群 $\overline{N} = N/U$, $\overline{N}$ 为初等交换 p-群. $\overline{G}$ 有极大子群 $\overline{M} = M/U$ 满足 $\overline{G} = \overline{M}\,\overline{N}$ 且 $\overline{M} \cap \overline{N} = 1$. 由假设 M 有完备 C 使得 $C/K(C)$ 循环且 $CM = G$. 令 $\overline{C} = CU/U$ 则 $\overline{G} = \overline{C}\,\overline{M}$, $\overline{C}$ 循环且 $\overline{C} \cap \overline{M} = 1$ (因为 $\overline{M}$ 是无核的). 推出 $|\overline{C}| = |\overline{N}|$. 再令 $\overline{P}$ 为 $\overline{G}$ 的一个 Sylow p-子群使得 $\overline{C}\,\overline{N} \leq \overline{P}$. 记 $\overline{X} = \overline{P} \cap \overline{M}$. 则 $\overline{P} = \overline{X}\,\overline{N} = \overline{X}\,\overline{C}$. 由此证明 $|\overline{N}| = 4$ (参阅 §7 引理 7.3, 也可直接引用此引理得 $|\overline{N}| = 4$).

4. 证明类似于定理 4.4.

§5.

1. 必要性显然. 反之设 M 为 G 的任一合数指数极大子群使得 $\eta(G : M)$ 无平方因子. 首先证明 G 可解. 设 N 为 G 的极小正规子群, 归纳得 G/N 可解. 若 N 非可解, 则 N 为同构的非交换单群的直积.

令 p 为 $|N|$ 的最大素数因子, $P \in \mathrm{Syl}_p(G)$. 由引理 1.11, 包含 $N_G(P)$ 的极大子群 M 在 G 中有合数指数. 同时, 由 Frattini 推论, $G = N_G(P)N = MN, \mathrm{Core}_G(M) = 1$. 所以 $\eta(G : M) = |N|$, 故 $|N|$ 无平方因子, 当然可解, 这是一个矛盾. 从而推出 G 为可解. 因为 G 的极大子群的指数均无平方因子, 故为素数, 由定理 1.12, G 为超可解.

2. 必要性显然. 充分性是定理 5.18 的直接推论.

3. 若 $\mathrm{Core}_G(M) \neq 1$, 应用归纳得出 G 可解. 故设 $\mathrm{Core}_G(M) = 1$. 令 N 为 G 的极小正规子群, 则 $\eta(G:M) = |N|$, 故 $|N|$ 为奇数, 由奇数阶群可解定理, N 为可解, 从而 G 为可解.

4. 类似第 3 题的证明.

5. 必要性. 设 G 可解, 则 $\eta(G:M) = |G:M|$, 当然 $\eta(G:M)/|G:M|$ 为 π-数.

充分性. 设 G 非可解, 令 N 为 G 的一个极小正规子群, 由归纳 G/N 为可解, 于是 N 为非可解. 因为 G 为 π-可解群, 所以 N 为 π'-群. 令 p 为 $|N|$ 的最大素因子, $P \in \mathrm{Syl}_p(N)$, 由引理 1.11, 包含 $N_G(P)$ 的极大子群 M 有合数指数. 又由 Frattini 推理, $G = MN$, 所以 $|G:M| = |N:M\cap N|$ 为 π'-数. 由假设 $\eta(G:M)/|G:M|$ 为 π-数, 但是 $\eta(G:M) = |N|$ 为 π'-数, 所以 $\eta(G:M) = |G:M|$, 由推论 5.14, G 为可解.

§6.

1. 见第 VIII 章习题第 7 题.

2. 令 P 为 G 的任一 Sylow 子群, 证明 P 的极小子群在 $N_G(P)$ 中正规. 如果 P 是 Sylow 2-子群, P 的 4 阶循环子群在 $N_G(P)$ 中也正规, 然后引用定理 6.8, 即得 G 为超可解.

3. 见第 VIII 章习题第 6 题.

4. 由上册第 V 章定理 4.5, 当 $\Phi(G) = 1$ 时, $F(G)$ 是初等交换群的直积, 由假设推出 $F(G)$ 的每个子群正规于 G, 再应用 §1 习题第 5 题即得 G 为超可解.

5. 假设 G 不是 2-幂零群, 则 G 包含一个子群 K 有如下性质: K 不是 2-幂零群而 K 的真子群皆为 2-幂零群. 由第 VIII 章定理 3.4, $|K| = 2^a p^b$, K 的 Sylow 2-子群为初等交换 2-群, 从而导出矛盾. 本题也可作为定理 6.7 的推论直接得出.

§7.

1. 参阅 §4 习题第 1 题的提示.

2. 设 G 为超可解, $H \leq G$. 令 $H_G = \mathrm{Core}_G(H), N/H_G$ 是 G 的一个主因子, 则 N/H_G 为循环群. 设 $N/H_G = \langle yH_G \rangle$, 则 $H < H\langle y \rangle = \langle y \rangle H$.

3. 令 $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ 是 G 的主列. 由定理 7.6, 每个 $|G_{i+1}/G_i|$ 是素数或 4. 假若对某个 $i, |G_{i+1}/G_i|$ 是大于 3 的素数 p, 而 $|G_i/G_{i-1}|$=2,3 或 4. 则 $G_i/G_{i-1} \leq Z(G_{i+1}/G_{i-1})$, 故 $G_{i+1}/G_{i-1} =$

$G_i/G_{i-1} \times \overline{G}_i/G_{i-1}$, 其中 $|\overline{G}_i/G_{i-1}| = p$ 而 $|G_{i+1}/\overline{G}_i| = 2, 3$ 或 4. 用 γ_i 代 G_i. 用这样的方法可得 G 的一个主列 $1 = \overline{G}_0 \le \overline{G}_1 \le \cdots \le \overline{G}_n = G$ 使得存在一个 s 满足当 $i \le s$ 时, $|\overline{G}_i/\overline{G}_{i-1}|$ 为大于 3 的素数, 而当 $i > s$ 时, $|\overline{G}_i/\overline{G}_{i-1}| = 2, 3$ 或 4, 从而导出结论.

4. 设 $H, K \trianglelefteq G$ 均为 G 的超可解嵌入子群, 令 $M = HK$, 则 $M \trianglelefteq G$. 根据约当定理 (上册第 III 章定理 1.5), 只要证 M 有 G-不变合成列 $1 = M_0 \le M_1 \le \cdots \le M_n = M$ 使得每个 M_i/M_{i-1} 为素数阶群. 当 $H \cap K = 1$, 这样的 G-合成列自然存在. 当 $H \cap K \neq 1$, 在 $H \cap K$ 中取 G 的极小正规子群 N. 则由条件 N 为素数阶, 由归纳, M/N 为 G/N 的超可解嵌入子群, 从而 M 为 G 的超可解嵌入子群.

5. 必要性显然. 设 $G/SE(G)$ 是 PC-群, 令 H 是 G 的任一子群. 若 $SE(G) \le H$, 因为 $G/SE(G)$ 是 PC-群, 存在一个 $y \notin H$ 使 $\langle y \rangle H = \langle y \rangle H$. 若 $SE(G) \not\le H$, 令 $1 = S_0 \le S_1 \le \cdots \le S_m = SE(G)$ 是 G-不变合成列使得所有因子群循环, 那么存在 $i < m$ 使得 $S_i \le H$ 而 $S_{i+1} \not\le H$. 记 $S_{i+1}/S_i = \langle yS_i \rangle$, 则 $\langle y \rangle H = H\langle y \rangle$. 因此 G 为 PC-群.

§8.

1. 参阅 Itô 的文章 On the degrees of irreducible representations of a finite groups. Nagoya Math. J. 3, 5 - 6(1951). 在这篇文章中, Itô 还证明, 如果群 G 的共轭类长的个数至多为 3, 则 G 可解.

2. 设 G 不是 p-群. 令 $x \neq 1$ 是任一 p'-元, 则 $|C_G(x)|$ 不是 p-幂, 故 $x \in Z(G)$. 于是 $G = P \times Z$, 其中 $1 \neq Z \le Z(G)$. 进一步证明 P 为交换即得 G 为交换群.

3. 设 p 为素数, 使得 $p^2 \mid |G|$. 令 $P \in \mathrm{Syl}_p(G)$, 则对 $\forall\, x \in P$, $|C_G(x)|$ 被 p^2 整除, 故 $x \in Z(G)$. 进一步证明每个 p'-元也 $\in Z(G)$.

4. 类似定理 8.8 的证明.

第 X 章

1. 由定义, $\mho_{i+1}(G) \le \mho_1(\mho_i(G)) \le \Phi(\mho_i(G)) < \mho_i(G)$.

2. 取 $G = \underbrace{Z_p \wr Z_p \wr \cdots \wr Z_p}_{e}$.

3. 证明 $Z_p \wr Z_p$ 可由 p 阶元素生成, 但其中含有 p^2 阶元.

4. 试找出 $G \times G$ 的一个具有非循环导群的二元生成子群, 再用定理 3.12(2).

5. 注意到二元生成的有限正则 3-群具有循环导群，再用对 s 的归纳法.

6. 这是一个学习运用换位子技巧的习题. 首先证明本题条件 $[g,h,h]=1, \forall g,h\in G$ 等价于 G 中任二共轭元均可交换，于是对 G 中任一元素 g, 有 g 的正规闭包 $g^G=\langle g^x \mid x\in G\rangle$ 是 G 的交换正规子群. 由此证明对于 G 中的一个简单换位子，如果其中有两项相同，则其值为 1. 我们用 $x_{1,2,\cdots,n}$ 简记 $[x_1,x_2,\cdots,x_n]$, 并依下列步骤证明若干换位子恒等式，从而得到本题的结论.

(1) $x_{1,3,2}=x_{1,2,3}^{-1}$: 因 $[x_1,x_2x_3]=x_{1,3}x_{1,2}x_{1,2,3}$, 得 $[x_1,x_2x_3]^{x_2}=x_{1,3}^{x_2}x_{1,2}^{x_2}x_{1,2,3}^{x_2}=x_{1,3}x_{1,3,2}x_{1,2}x_{1,2,3}$ 和 $[x_1,x_2x_3]^{x_2x_3}=x_{1,3}^{x_3}x_{1,3,2}^{x_3}x_{1,2}^{x_3}x_{1,2,3}^{x_3}=x_{1,3}x_{1,3,2}x_{1,2}x_{1,2,3}^2$. 但 $[x_1,x_2x_3]^{x_2x_3}=[x_1,x_2x_3]$, 于是 $x_{1,2}=x_{1,3,2}x_{1,2}x_{1,2,3}$. 又 $x_{1,2}$ 与 $x_{1,2}x_{1,2,3}$ 可交换，即得结论.

(2) 对任意的 $x,y\in G$ 有 $[x^{-1},y]=[x,y^{-1}]=[x,y]^{-1}$: 用共轭元素可交换来证明.

(3) $x_{1,2,3}=x_{2,1,3}^{-1}$: 用 (2) 式来证明.

(4) $x_{1,2,3}^3=1$: 由 Witt 公式证明 $x_{1,2,3}^{-1}x_{2,3,1}^{-1}x_{3,1,2}^{-1}=1$, 再用 (1), (3) 两式.

至此已证若 G 中无 3 阶元素，则 G 幂零且 $c(G)<3$. 下面设 G 中有 3 阶元素.

(5) $x_{1,2,3,4}=x_{1,2,4,3}^{-1}$: 用 $x_{1,2}$ 代替 (1) 式中的 x_1, 用 x_3 和 x_4 分别代替 (1) 式中的 x_2 和 x_3, 由 (1) 即得.

(6) $x_{2,1,3,4}=x_{1,2,3,4}^{-1}$: 用 (3) 和 (2), 略.

(7) $x_{1,3,2,4}=x_{1,2,3,4}^{-1}$: 用 (1) 和 (2), 略.

因为 (1 2), (2 3), (3 4) 生成 S_4, 故对 $x_{1,2,3,4}$ 的脚标作任意置换，都得到 $x_{1,2,3,4}$ 或其逆，依赖于该置换是偶置换还是奇置换.

(8) $x_{1,2,3,4}^2=1$: 由 (1) 和 (3), $x_{1,2,3,4}=[x_{1,2},x_3,x_4]=[x_3,x_4,x_{1,2}]=[x_{3,4},x_{1,2}]$. 同理 $x_{4,3,1,2}=[x_{1,2},x_{3,4}]=[x_{3,4},x_{1,2}]^{-1}=x_{1,2,3,4}^{-1}$. 但 $x_{1,2,3,4}=x_{3,4,1,2}$, 故得结论.

(9) $x_{1,2,3,4}^3=1$: 在 (4) 中用 $x_{1,2}$ 代替 x_1, 而用 x_3, x_4, 分别代替 x_2, x_3 即得.

最后由 (8) 和 (9) 即得 $x_{1,2,3,4}=1$.

7. 首先证明由 $(xy)^3=1, \forall x,y\in G$, 可推出 $yxyx^{-1}=xyx^{-1}y$, 即 G 中任二共轭元素可交换，于是由上题知 G 中成立 $[g,h,h]=1, \forall x,y\in G$, 并且 G 是幂零群，且 $c(G)\le 3$. 由此推出 G 是亚交换群.

设 G 由 $\{x_1,\cdots,x_d\}$ 生成. 证明 G'/G_3 可由 $\{[x_i,x_j] \mid i\neq j\}$ 生成，其中共有 $\binom{d}{2}$ 个生成元. 再由上题提示中 (1) 和 (3) 知 $[x_i,x_j,x_k]$ 和 $[x_s,x_t,x_r]$ 生成同一子群，只要集合 $\{i,j,k\}=\{s,t,r\}$. 于是 G_3 至多有 $\binom{d}{3}$ 个生成元. 这就得到 $|G|\le 3^d+3^{\binom{d}{2}}+3^{\binom{d}{3}}$.

为证上面的界确实能够达到，试用群扩张理论构造出所需的群.

8. 参照引理 2.8 的证明. 必要时参看下列论文中的定理 2:

A. Mann, Regular p-groups, *Israel J. Math.*, **10**(1971), 471–477.

9. 如果 $\exp(G)=p$, 则 G 当然正则. 于是可设 $\exp(G)>p$. 在 $\mho_1(G)$ 中取一 p 阶正规子群 N, 考虑商群 $\overline{G}=G/N$. 证明 $\overline{G}$ 仍满足本题的条件，于是 $\overline{G}$ 正则. 由 $N\le\mho_1(G)$ 推出 $p^{\omega(G)}=|G/\mho_1(G)|=|\overline{G}/\mho_1(\overline{G})|=|\Omega_1(\overline{G})|\le p^{p-2}$, 由定理 2.7 即得结论.

10. 只须证必要性. 设 G 是极小反例，则 $c(G)=p$ 且 $|G_p|=p$. 设 $G=\langle A,g\rangle$, 其中 A 是 G 的交换极大子群. 则 G_i/G_{i+1} 可由形如 $[a,\underbrace{g,\cdots,g}_{i-1}]$ 的换位子生成. 注意到这时有 $G'=[G,A]$, 推出 $\mho_1(G')=1$, 于是 G 是 p-交换的，有 $(ga)^p=g^pa^p$. 再应用亚交换群中的换位子公式直接计算得 $(ga)^p=g^pa^p[a,\underbrace{g,\cdots,g}_{p-1}]$. 因此 $[a,\underbrace{g,\cdots,g}_{p-1}]=1$, 得到矛盾.

11. 设 G 是极小反例. 考察 G 的真子群 H, 区分 H 包含 N 和不包含 N 两种情形，证明 H 都是正则的. 再考察 G 的真商群 G/K, 区分 $K\cap N=1$ 和 $K\cap N\ne1$ 两种情形，证明 G/K 都是正则的. 于是 G 是极小非正则 p-群. 证明极小非正则 p-群只有唯一的极小正规子群，从而推出矛盾.

12. 参看下列论文中的命题 10 和命题 11:

A. Mann, Regular p-groups II, *Israel J. Math.*, **14**(1973), 294–303.

13 – 16. 参看下列论文:

A. Mann, Regular p-groups III, *J. Algebra*, **70**(1981), 89–101.

17 – 19. 参看下列论文，但要注意该文中使用的符号和术语与我们的有所不同.

W. Bannuscher, Über k-Φ-reguläre p-Gruppen, *Math. Nachr.*, **137**(1988), 7–17.

20. 设 G 是极小非亚循环 p-群. 若 $\Phi(G)=1$, 则 G 是 p^3 阶初等交换群. 若 $\Phi(G)\ne1$, 则 G 必为二元生成群，并且是非交换群. 由定理 5.2 知 $\Phi(G')G_3=1$, 于是 $|G'|=p$. 若 $p>2$, 证明 G 是 p^3 阶且方次数为 p 的非交换群. 若 $p=2$, 证明不存在这样的群.

21. 应用亚交换群幂零类的估值，用对 r 的归纳法.

第 XI 章

1. (2) 令 $A_i=\{\alpha|x_i^\alpha=a_\alpha x_i, x_j^\alpha=x_j, j\ne i, a_\alpha\in\mathbf{F}^\#\}$, $i=1,2,3$. 证明 $G_{(\Delta)}=A_1\times A_2\times A_3\cong Z_3\times Z_3\times Z_3$. 记 $\mathbf{B}_{ij}=\mathbf{I}_4-\mathbf{E}_{ii}-\mathbf{E}_{jj}+\mathbf{E}_{ij}+\mathbf{E}_{ji}$. 证明 $G_{\{\Delta\}}=\langle G_{(\Delta)},\mathbf{B}_{ij}|i\ne j,1\le i,j\le4\rangle$, $G_{\{\Delta\}}/G_{(\Delta)}\cong S_4$.

类似地可证 (2) 中其它结论.

2. (2) (ii) 假定 $x \in V$, $(x,x) \neq 0$. 令 $(x,x) = a$. 作半线性型: $[z,y] = a^{-1}(z,y)$. 显然 $[\ ,\ ]$ 相似于 $(\ ,\ )$. 又 $[x,x] = 1$, 仍将 $[\ ,\ ]$ 记为 $(\ ,\ )$.

令 $w = (y,x)z - (z,x)y$. 则 $(x,w) = 0 \Longrightarrow 0 = (w,x) = (y,x)^{\theta}(x,z) - (z,x)^{\theta}(x,y)$. 令 $x = y$, 则得 $(x,z) = (z,x)^{\theta}$, $\forall z \in V$. 类似于以上讨论, 可证: $\forall y,z \in V$, $(y,z) = (z,y)^{\theta}$. 这就证明了 $(\ ,\ )$ 相似于一个 Hermite 型.

(iii) 设 $(u,u) \neq 0$, $V = \langle u \rangle \oplus u^{\perp}$. 我们证明 $u^{\perp}$ 为全迷向的. 先证 $(v,v) = 0$, $\forall v \in V$. 假定相反, 即存在 $v \in V$, 使 $(v,v) \neq 0$. 取 $b = -(u,u)/(v,v)$. 则 $(u+bv, u+v) = 0$. 由假定, $0 = (u+v, u+bv) = (u,u) + b(v,v)$. 若 $b \neq b^{\theta}$, 即得出矛盾. 若 $b = b^{\theta}$, 则由于 $o(\theta) > 2$, 故存在 $a \in \mathbf{F}^{\#}$, 使 $aa^{\theta} \neq (aa^{\theta})^{\theta}$. 以 au 代替 u, 再如上讨论即得矛盾.

类似以上讨论, 可证明 $u^{\perp}$ 全迷向, 故 $u^{\perp} \subseteq R(V)$.

5. (3) 令 $H = G\langle x \rangle, x \in N_H(S)$. 由 Schur-Zassenhaus 定理, S 在 S 在 $N_G(S)$ 中的补的集合上传递作用, 故 x 正规化 S 在 $N_G(S)$ 中的某个补, 假定为 K. 我们有 $[K,S,x] = [S,x,K] = 1$, 由三子群引理有 $[x,K,S] = 1$. 由 (2), $[k,K] = 1$, 从而有 $[x, N_G(S)] = 1$. 又由 (2), K 恰正规化另一 Sylow p-子群 T, 从而 x 正规化 T. 由于 x 平凡作用在 S 在 $N_G(G)$ 中的任意补上, 故由 (1), x 正规化 G 的所有 Sylow p-子群, 从而 x 属于 H 在 $\mathrm{Syl}_p(G)$ 上作用的核 M 之中, 由于 $G/Z(G)$ 为单, 故 $M \cap G = Z(G)$. 又因 $G = G'$, 再次利用三子群引理即得 $[x,G] = 1$, 这就证明了 $x = 1$.

8. (2) 若 $H \cong A_8$, 则 H 中有生成元 $\{g_i | 1 \leq i \leq 6\}$ 并且有如下定义关系: ${g_1}^3 = {g_i}^2 = 1\ (2 \leq i \leq 6)$, $(g_i g_{i+1})^3 = 1\ (1 \leq i \leq 5)$, $(g_i g_j)^2 = 1\ (1 \leq i \leq 4; i+1 < j)$.

令 $G = GL(4,2) = PSL(4,2)$, 由令

$$\tilde{g_1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \qquad \tilde{g_2} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

$$\tilde{g_3} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \tilde{g_4} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

$$\tilde{g_5} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \tilde{g_6} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

可证 $\{\tilde{g_i} \mid 1 \le i \le 6\}$ 与 H 中的 $\{g_i \mid 1 \le i \le 6\}$ 满足相同的关系.

9. (2) 这一问题可通过以下步骤证明.

(i) 设 $g \in G$, 则存在 $h \in H$, 使 $g^h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(ii) 若 g_1, g_2 为 G 中两个互相不可交换的 p-阶元, 则可找到 $h \in H$, 使

$$g_1^h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad g_2^h = \begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}.$$

由 (i), 可假定 g_1 和 g_2 具有形状:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad 和 \quad S^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}S.$$

要完成 (ii) 的证明, 仅需证: 可选取 S, 使之具有形状 $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$.

(iii) 令 $g_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $g_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. 则

$$S_1 = C_G(g_1) = \left\{ \begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix} \middle| e \in \mathbf{F} \right\} \in \mathrm{Syl}_p(G),$$

$$S_2 = C_G(g_2) = \left\{ \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix} \middle| f \in \mathbf{F} \right\} \in \mathrm{Syl}_p(G).$$

(a) 设 $\eta \in \mathrm{Aut}(G)$, 则由 (ii), 可假定

$$g_1^\eta = g_1, \qquad g_2^\eta = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}.$$

这表明 $S_1^\eta = S_1$, $S_2^\eta = S_2$.

(b) 记 $t = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 证明: $t^\eta = t$.

由于 $S_1^t = S_2$, 又由 (i) $S_1^{t^\eta} = S_2$, 故 $t^\eta \in G$ 具有形状 $\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}$.

利用关系式 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = g_1 \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} g_1$, 比较两端在 η 之下的象可得 $t^\eta = t$.

(c) 由 $S_1^\eta = S_1$ 可得 $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^\eta = \begin{pmatrix} 1 & x^\sigma \\ 0 & 1 \end{pmatrix}$. 可验证: $1^\sigma = 1$, $(x+y)^\sigma = x^\sigma + y^\sigma$. $\forall x, y \in \mathbf{F}$. $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}^\eta = \begin{pmatrix} 1 & 0 \\ x^\sigma & 1 \end{pmatrix}$.

(d) 证明 $\sigma \in \mathrm{Aut}(\mathbf{F})$. 为此证 $\forall x, y \in \mathbf{F}^\#$, $(x^{-1})^\sigma = (x^\sigma)^{-1}$, $(xy)^\sigma = x^\sigma y^\sigma$.

我们有 $N_G(S_1) \cap N_G(S_2) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \middle| x \in \mathbf{F}^\# \right\}$,

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x^{-1} & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}.$$

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}^\eta = \begin{pmatrix} 1 & -x^\sigma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (x^{-1})^\sigma & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x^\sigma & 1 \end{pmatrix}.$$

由于 $N_G(S_1) \cap N_G(S_2)$ 在 η 作用下不变, 即得 $(x^{-1})^\sigma = (x^\sigma)^{-1}$. 又利用上述结果立得 $\begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}^\eta = \begin{pmatrix} x^\sigma & \\ & (x^{-1})^\sigma \end{pmatrix}$. 由此可得 $(xy)^\sigma = x^\sigma y^\sigma$. 故 $\sigma \in \mathrm{Aut}(\mathbf{F})$. 由于 $G = \langle S_1, t \rangle$, 故有 $g^\eta = g^\sigma$, $\forall g \in G$. 这就完成了证明.

10. (1) 设 p 为 $|Z(G)|$ 的一个素因子.

(i) 若 $p \neq 2$, 则由 Frobenius 正规 p-补定理, 立得矛盾. 这表明 $Z(G)$ 为 2-群.

(ii) 设 $P \in \mathrm{Syl}_2(G)$. 则 $P/Z(G) \cong Z_2 \times Z_2$. 设 $D \le N_G(D)$, $|D| = 3$. 记 $\widetilde{P} \cong [P, D]$. 证明 $D, \widetilde{P}$ 满足 Hall-Higman 简化定理的条件, 并从而证明 $\widetilde{P} \cong Q_8$.

此外, 不难证明 $P = \widetilde{P}$.

(iii) $SL(2,5)$ 可由如下矩阵生成:

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

证明 G 中有生成元 $\tilde{x}, \tilde{y}$, 且 $\tilde{x}, \tilde{y}$ 满足下列条件: $\tilde{x}^5 = \tilde{y}^3 = (\tilde{x}\tilde{y})^2 = 1$. 由此证明 $G \cong SL(2,5)$.

第 XII 章

11. 考虑群元素的子集合 $S_1 = \{g \mid \alpha^g \in \Gamma\}$ 和 $S_2 = \{g \mid \beta^g \in \Delta\}$. 设 $S_1 \subseteq S_2$, 推出矛盾.

13. 设 $\Delta_i(\alpha)=\Gamma$. 考虑路 α',β',γ', 其中 $(\beta',\alpha'),(\beta',\gamma')\in\Delta_i$ 但 $\alpha'\neq\gamma'$. 称 α',β',γ' 为一个 Θ-路. 证明 G 在全部 Θ-路上传递.

14. 由推论 4.13(3) 知 $\Delta_1(\alpha)$ 长为 p. 考虑 Δ_1 决定的交错路. 令 $\Gamma=\Delta_1(\alpha)\cup\{\alpha\}$. 证明 $G_{(\Gamma)}$ 的阶与 p 互素.

15. 考虑有序对 (α,x), 其中 $x\in K$ 而 $\alpha\in \mathrm{fix}_{\Omega}(x)$. 计算这种对的个数.

16. 考虑 $(x,\{\alpha,\beta\})$, 其中 x 为对合, 而 x 的轮换分解式中有 (α,β).

20. 证明 G 中包含 3-轮换.

23. 以 168 阶单群为例, 计算 G 中 Sylow 7-子群的个数 n, 证明 G 有 n 级本原表示, 并具体构造这样的本原群. 对 660 阶单群同样处理.

27. 考虑 G 在 Ω 的 2 元子集的集合 $\{\{\beta,\gamma\}\mid\beta\neq\gamma\in\Omega\}$ 上和在集合 $\{(\alpha,\{\beta,\gamma\})\mid\alpha,\beta,\gamma\in\Omega,\ \alpha,\beta,\gamma \text{ 互不相等}\}$ 上的作用.

30. 利用条件 $G\not\geq A_\Omega$ 证明 G 中没有 7-轮换和 5-轮换, 继而证明 G 为精确 4-传递的.

第 XIII 章

4. (1) (ii) $P_s\cap sP_s=\varnothing$ 是显然的.

要证 $W=P_s\cap sP_s$, 只需证: 若 $w_1\notin P_s$, 则 $w_1\in sP_s$.

由于 $w_1\notin P_s$, 则 $l(sw_1)\leq l(w_1)$. 设 $w_1=s_1\cdots s_q$, 则由交换性条件可证 $w_1\in sP_s$.

(iii) 由 (iii) 中假定及 (ii) 可知 $ws'\in sP_s$, 故有 $l(sws')\leq l(ws')$, 并从而得 $l(w)\leq l(ws')$.

令 $w=s_1\cdots s_q$ 为 w 的最短表达式. 则 $s_1\cdots s_qs'$ 为 ws' 的最短表达式. 利用交换性条件即得结论.

(2) 假定 $w\notin P_s$, $w=s_1\cdots s_q$ 为 w 的最短表达式. 由 (i) 可知, 存在 j 使 $s_1\cdots s_{j-1}\in P_s$, $s_1\cdots s_j\notin P_s$ 由 (iii), $s_1\cdots s_j=ss_1\cdots s_{j-1}$. 故有 $l(sw)<l(w)$.

又若 $\tilde{w}\in P_s$, 则 $s\tilde{w}\in sP_s$, 从而由 (ii), $s\tilde{w}\notin P_s$, 故有 $l(\tilde{w})<l(s\tilde{w})$.

由以上讨论, 我们即可证明 (W,S) 满足交换性条件.

6. 若 $s\in J, r\in S\backslash J$, 则 $Bs\cap H\neq\varnothing$, 且由 $H\trianglelefteq G$ 可知 $rBsr\cap P_J\neq\varnothing$. 故存在 $w\in W_J$ 使 $Bsr\cap rBwB\neq\varnothing$.

由定义 4.1(T3), 必有 $sr=rw$. 又由命题 4.4(1) 可知 $l(w)=1$, 特别地 $w\in S$. 又由定理 4.6 知, S 可以看作是一个厦中的某个寓的一个室中所有墙的反射之集合. 考虑到 S 在该室中诸顶点上的作用, 立知 $w=s$. 这就证明了 $sr=rs$.

7. 可通过以下步骤完成本题的证明.

(1) $b=b_\alpha=1$.

假定 $b>1$, 则 $b\geq 3$. 注意由题设 α' 必共轭于 β.

(i) 首先假定 $\forall\alpha-1\in\Delta(\alpha)\setminus\{\beta\}$, $\lambda\in\Delta(\alpha')\setminus\{\alpha'-1\}$, 总有 $Z_{\alpha-1}\leq Q_{\alpha'-1}$, $Z_\lambda\leq Q_\beta$.

证明: $[V_\alpha, Z'_\alpha]\leq Z_\alpha$, 由此推出 $Z_\alpha Z_\beta\trianglelefteq G_\alpha$, 类似地证明 $Z_\lambda Z_{\alpha'}\trianglelefteq G_{\alpha'}$, 由 α' 共轭于 β, 得出 $Z_\beta Z_\alpha\trianglelefteq G_\beta$, 立得矛盾.

(ii) 假定存在 $\alpha-1\in\Delta(\alpha)\setminus\{\beta\}$, 使 $Z_{\alpha-1}\not\leq Q_{\alpha'-1}$. 证明必存在 $\alpha-2\in\Delta(\alpha-1)$, 使 $Z_{\alpha-2}\not\leq Q_{\alpha'-2}$.

(iii) 令 $R=[Z_\alpha, Z_{\alpha'}]$, 由 (ii) 可证 $[R, G_{\alpha'-1}]=[R, G_{\alpha'-2}]=1$, 矛盾.

(i) – (iii) 证明了 $b=b_\alpha=1$.

(2) $Q_\alpha\cong S_4\cong Q_\beta$ 或 $Q_\alpha\cong S_4\times Z_2\cong Q_\beta$.

(i) $\Phi(Q_\alpha)=\Phi(Q_\beta)=1$: 由 $b=1$, 故 $Q_\alpha=Z_\alpha(Q_\alpha\cap Q_\beta)$, $Q_\beta=Z_\beta(Q_\alpha\cap Q_\beta)$, 于是有 $\Phi(Q_\alpha)=\Phi(Q_\alpha\cap Q_\beta)=\Phi(Q_\beta)$, 由此立得结论.

(3) 证明 $Q_\alpha=[Q_\alpha, d_1]\times\Omega_1(Z(G_\alpha))$, $Q_\beta=[Q_\beta, d_2]\times\Omega_1(Z(G_\beta))$, 其中 $d_1\in G_\alpha$, $d_2\in G_\beta$, $o(d_1)=o(d_2)=3$. 又 $[Q_\alpha, d]\cong Z_2\times Z_2\cong[Q_\beta, d]$, $|\Omega_1(Z(G_\alpha))|=|\Omega_1(Z(G_\beta))|\leq 2$.

(iii) 若 $\Omega_1(Z(G_\alpha))=\Omega_1(Z(G_\beta))=1$, 证明 $G_\alpha\cong S_4\cong G_\beta$. 若 $|\Omega_1(Z(G_\alpha))|=|\Omega_1(Z(G_\beta))|=2$, 证明 $G_\alpha\cong S_4\times Z_2\cong G_\beta$.

第 XIV 章

§1.

2. 用反证法. 设 $|\mathrm{Aut}(X)|$ 为偶数, 则存在二阶自同构 $\alpha\in\mathrm{Aut}(X)$. 设 $(u\ v)$ 是 α 的轮换分解式中的一个对换, 则必有 (u,v) 和 (v,u) 均为 X 的弧, 与 X 是竞赛图相矛盾.

§2.

2. 直接计算二图的邻接矩阵和它们的特征多项式.

3. 应用 Cauchy-Schwarz 不等式于 $(\lambda_2,\cdots,\lambda_n)$ 和 $(1,\cdots,1)$.

§3.

3. $\mathrm{Aut}(P_n)\cong Z_2$ 且 $\mathrm{Aut}(C_n)\cong D_{2n}$. 对于 P_n, 仅当 $n=2$ 时是点传递, 边传递和弧传递的; 而对于 C_n, 只要 $n\geq 3$, 就是点传递, 边传递且弧传递的.

4. 对于 $n \neq 4$, $\mathrm{Aut}(C_n[2K_1]) = Z_2 \wr D_{2n}$, 其中 D_{2n} 看成是 n 个点上的置换群; 对于 $n = 4$, $C_4[2K_1] \cong K_{4,4}$, 因此 $\mathrm{Aut}(C_4[2K_1]) = \mathrm{Aut}(K_{4,4}) = S_4 \wr Z_2$. 对于所有情形, 图 $C_n[2K_1]$ 都是点传递, 边传递和弧传递的.

5. 对于 $n \neq 4$, $\mathrm{Aut}(C_n \times K_2) = D_{2n} \times Z_2$; 这时图 $C_n \times K_2$ 是点传递的, 但不是边传递和弧传递的. 对于 $n = 4$, $\mathrm{Aut}(C_4 \times K_2) = S_4 \times Z_2$. 首先, 众所周知, 正立方体在三维欧氏空间的对称群是 S_4, 再加上反射, 图的全自同构群应为 S_4 被 Z_2 的扩张. 因为 S_4 是完全群, 这个扩张一定是直积. 容易验证, 这时图 X_4 是点传递, 边传递和弧传递的.

8. 把 Q_n 的顶点集合看成是 $GF(2)$ 上 n 维向量空间, 它的加法群同构于 Z_2^n, 可看成是 $A = \mathrm{Aut}(Q_n)$ 的子群. 以 0 表零向量代表的顶点. 则 0 的邻域 N 是向量空间的一组基. 因此 N 的任一置换都诱导出图 Q_n 的一个自同构. 于是 $\mathrm{Aut}(Q_n) \geq Z_2^n \rtimes S_n$. 再证明对于任意的 $\alpha \in \mathrm{Aut}(Q_n)$, 只要 α 不动 $N \cup \{0\}$ 中的任意顶点, 则不动图 Q_n 的每个顶点, 于是 $\mathrm{Aut}(Q_n) = Z_2^n \rtimes S_n$. 最后据上题 (2), 得 Q_n 的 2-弧传递性.

9. (2) 用左面的图示证明 Petersen 图是点传递的. 再用第 7 题 (2) 及右面的图示首先证明它是 2-弧传递的. 然后考虑一个取定的 2-弧的稳定子群, 在其中寻找一个图自同构使得与此 2-弧的端点相邻接的两个顶点互变, 从而 Petersen 图是 3-弧传递的.

10. 我们只提示证明图的点本原性, 即证明 $S_{n-2} \times S_2$ 是 S_n 的极大子群. 为此, 设 G 是 S_n 的任一真包含 $S_{n-2} \times S_2$ 的子群. 则显然 G 在 $\Omega = \{1, 2, \cdots, n\}$ 上传递, 并易证 G 在 Ω 上本原. 用第 XII 章推论 6.3 得 $G = S_n$, 于是 $S_{n-2} \times S_2$ 是 S_n 的极大子群.

11. 我们也只提示证明图的点本原性, 但用不同于上题的方法. 考虑群 $G = P\Gamma L(n, q)$ 在 V 的二维子空间的集合上的作用. 这个作用是传递的. 证明 G 的秩为 3, 即 G 只有两个非平凡的轨道图, 其中的一个就是本题所定义的图, 另一个图的邻接关系由 $B \sim C \iff \dim(B \cap C) = 1$ 来确定. 证明这两个图都是连通的, 于是由第 XII 章定理 4.4 得 G 的本原性.

§4.

1. 穷举所有的 6 阶点传递图.

2. 证明 p 阶点传递图的自同构群的 Sylow p-子群就是 Z_p, 它是自同构群中的正则子群. 用命题 4.3.

3. 证明一个置换群的结果, 由它立得本题的结论. 这个结果是: 任一 p^2 级的极小传递置换群必为正则群. (所谓极小传递群指的是本身传递但它的每个真子群都不传递的置换群.)

设 G 是 p^2 级极小传递群. 因为 p^2 级传递群的 Sylow p-子群仍传递, 故 G 本身为 p-群. 令 M 为 G 的任一极大子群, 则 M 非传递. 对任一

$v \in V$, 我们有 $|G_v| = |G|/p^2$, 以及 $|M_v| > |M|/p^2$, 于是 $M_v = G_v$. 由此有 $G_v \le M$. 由 M 的任意性, 有 $G_v \le \Phi(G)$. 若 $|G : \Phi(G)| = p$, 则 G 循环, 因此 G 正则. 若 $|G : \Phi(G)| = p^2$, 则 $G_v = \Phi(G)$. 因 $\Phi(G) \trianglelefteq G$, 又 G_v 作为传递置换群的点稳定子群是无核的, 我们有 $G_v = 1$, 并因此有 $G \cong Z_p^2$ 是正则的.

5. 由上题只须证 D_6 是 2-DCI-群. 设 $D_6 = \langle a, b \mid a^3 = 1, b^2 = 1, bab = a^{-1}\rangle$. 我们考察 D_6 的所有一元子集的集合和二元子集的集合在 $\mathrm{Aut}(D_6) \cong D_6$ 作用之下的轨道. 容易看出, $\mathrm{Aut}(D_6)$ 在一元子集上有两个轨道, 它们可以 $\{a\}$ 和 $\{b\}$ 为代表; $\mathrm{Aut}(D_6)$ 在二元子集上有三个轨道, 它们可以 $\{a, a^{-1}\}$, $\{b, a\}$ 和 $\{b, ba\}$ 为代表. 由验证知属于不同轨道的子集决定的 Cayley 有向图彼此互不同构, 因此 D_6 是 2-DCI-群.

6. 由第 4 题只须证 Q_8 是 3-DCI-群, 方法同上题提示.

7. 因为 $G = Z_n$ 循环, 由定理 4.13, G 是 1-DCI-群. 为证 G 为 2-DCI 的, 任给 G 的两个二元子集 $S = \{a, b\}$ 和 $T = \{a', b'\}$, 满足 $X = \mathrm{Cay}(G, S)$ 和 $X' = \mathrm{Cay}(G, T)$ 同构, 我们要证明存在 $\alpha \in \mathrm{Aut}(G)$ 使得 $S^\alpha = T$.

首先给出一些符号. 对于 Cayley 有向图 $X = \mathrm{Cay}(G, S)$, 设 $x \in G$, i 为任一正整数, 我们令

$$X_i(x) = \{y \in G \mid \text{在 } X \text{ 中存在由 } x \text{ 到 } y \text{ 的长为 } i \text{ 的有向途}\}.$$

显然, $X_1(x) = xS = \{xa, xb\}$, $X_2(x) = xS^2 = \{xa^2, xab, xb^2\}$.

设 $\sigma : X \to X'$ 是图同构, 且满足 $1^\sigma = 1$. 于是 $S^\sigma = T$. 我们还不妨设 $a^\sigma = a'$, $b^\sigma = b'$. 考虑集合 $X_2(1) = \{a^2, ab, b^2\}$. 有两种情况: (1) $|X_2(1)| = 3$, 即 $a^2 \ne b^2$; (2) $|X_2(1)| = 2$, 即 $a^2 = b^2$.

对于情形 (1), 注意到 ab (或 $a'b'$) 是 $X_1(a) \cap X_1(b)$ (或 $X_1'(a') \cap X_1'(b')$) 中的唯一的元素, 故 $(ab)^\sigma = a'b'$, 并因此 $(a^2)^\sigma = a'^2$, $(b^2)^\sigma = b'^2$. 用对 $i + j$ 的归纳法即可证明 $(a^i b^j)^\sigma = a'^i b'^j$, $\forall i, j$. 这样, σ 就是所求的群同构.

对于情形 (2), $a^2 = b^2$, 因此也有 $a'^2 = b'^2$. 于是 $u := a^{-1}b = a'^{-1}b'$ 是 G 中唯一的 2 阶元. 由图同构得 $|\langle S\rangle| = |\langle T\rangle|$, 于是 $o(a) = o(a')$. 这样就存在所需的群同构 τ 使 $a^\tau = a'$, 从而 $S^\tau = T$.

8. 在本题条件下, 有 $\varphi(n) > 2$, 于是存在 c 满足 $2 \le c \le n - 2$. 考虑 G 的下列子集:

$$\begin{aligned} A &= \{n, -n\}, \quad B = \{kn + 1, kn - 1 \mid 0 \le k \le n - 1\}; \\ H &= A \cup B, \\ K &= cA \cup B. \end{aligned}$$

验证 $\mathrm{Cay}(G, H) \cong \mathrm{Cay}(G, K)$, 但不存在 $\alpha \in \mathrm{Aut}(G)$ 使 $H^\alpha = K$.

9. 参看下文 §4:

L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29**(1977), 329–336.

10. 因为任意图和它的补图具有相同的自同构群, 故只须考虑度数 ≤ 3 的情况. 然后再分别对连通和不连通两种情况进行讨论. 对不连通情况, 自同构群是两个阶较小的群的圈积; 而对连通的情况, 图同构于 Q_3.

11. 参看上题提示.

12. 参看第 10 题提示.

§5.

1. 参看第 XII 章例 4.15.

2. 参看第 XII 章例 4.17.

3. 分别度数为 0 到 5 来讨论. 它们是 $6K_1$, $3K_2$, $2K_3$, C_6, $K_{3,3}$, $K_3 \times K_2$, $K_6 - 3K_2$ 和 K_6.

4. 不连通情况是若干彼此同构的 ≤ 4 阶的对称图的并, 因此可只考虑连通的情况. 设 $X \neq K_8$ 是这样一个 8 阶对称图, 设 $A = \mathrm{Aut}(X)$. 由第 XII 章例 4.16 知 A 非本原. 区别极小的非本原集的不同长度, (它们是 2 或 4), 来定出可能的商图. 对于每个商图 $\overline{X}$, A 诱导出商图的一个自同构群 $\overline{A} = A/K$, 其中 K 是 A 在完全非本原系上作用的核. 分别 K 在诸块上作用传递或非传递来讨论原图 X 的可能的结构, 从而定出 X.

5. 假定 X 是一个 13 阶的对称图, $X \neq K_{13}$, $13K_1$. 证明 X 必为 Z_{13} 的正规 Cayley 图. 令 $X = \mathrm{Cay}(Z_{13}, S)$, 则 $\mathrm{Aut}(Z_{13}, S)$ 在 S 上作用传递. 证明 S 必为 $\mathrm{Aut}(Z_{13})$ 的一个偶阶子群的的陪集.

6 – 7. 参看上题提示.

§6.

1. 设 $X = \mathrm{Cay}(G, S)$ 是交换群 G 的无向 Cayley 图. 对任意的 $(g, sg) \in E(X)$, 只须证明存在 $\alpha \in \mathrm{Aut}(X)$ 使 $(g, sg)^\alpha = (sg, g)$. 因为 $\sigma : g \mapsto g^{-1}$, $\forall g \in G$, 是群 G 的自同构且不变 S, 因此 $\sigma \in \mathrm{Aut}(X)$. 令 $\alpha = \sigma R(sg^2)$ 即可.

2. 仿照上题提示.

索 引

(以汉语拼音为序)

T

W

X